MASTER EN SCIENCES INFORMATIQUES

Analyse de risques dans le cadre d'une application distribuée sur l'Internet

Hislaire, Olivier

Award date:
2003

FACULTÉS UNIVERSITAIRES NOTRE-DAME DE LA PAIX, NAMUR

INSTITUT D'INFORMATIQUE

RUE GRANDGAGNAGE, 21, B-5000 NAMUR (BELGIUM)

Analyse de risques dans le cadre d'une application distribuée sur l'Internet

Olivier Hislaire

Mémoire présenté en vue de l'obtention du grade de

Licencié en Informatique

Année Académique 2002 - 2003

Résumé

Ce document retrace une démarche, celle d'une étude de sécurité menée comme préalable à la prise de décision initiale pour un projet *d'application de communication vocale via l'Internet*.

Nous avons suivi, dans cette étude, une démarche en cinq étapes. Après la présentation générale du contexte et des objectifs, nous avons tenté d'établir nos besoins de sécurité puis d'identifier les menaces significatives. Au cours de la quatrième étape, nous avons sommairement investigué quelques réponses technologiques possibles à certains de nos besoins de sécurité, pour ensuite terminer ce travail par des propositions de spécification fonctionnelle, d'architecture et de mode d'acquisition du produit.

Et aboutir, finalement, à la décision de démarrer le projet, ou pas.

Mots clés: *Sécurité, VoIP*

Abstract

This document concerns a process, the process of a risk analysis conducted as a preliminary step before we even decide to start on with our *internet-enabled vocal communication system* project.

To achieve this we used a five steps approach. After a short discussion of the project context and main objectives, we first established the related security needs before we could try and identify the main threats. During the fourth step, we briefly investigated some technological issues that could be considered as possible answers to our security needs, before we conclude with some proposals concerning the product functional specification, architecture and *buy or build* dilemma.

Which finally lead us to the *go/no go* decision.

Keywords: *Security, VoIP*

Avant-propos

Arrivé au terme de cette étude, il m'est particulièrement agréable d'exprimer ma reconnaissance à tous ceux qui, de près ou de loin, lui ont permis de voir le jour.

Je pense tout particulièrement à Mr Jean Ramaekers, promoteur de ce mémoire dont la disponibilité, les critiques discrètes mais toujours judicieuses, les précieux conseils, la patience et les encouragements m'ont été fort utiles durant toutes les étapes de ce travail.

Merci aussi à mes collègues de cours pour leur exemple et leurs encouragements, ainsi qu'à mon cher et vieil ami Jacques Delhaye dont le sens critique, plus aiguisé que jamais, m'a été plus d'une fois bien utile. Merci encore à vous, membres du Jury, de l'intérêt que vous voudrez bien porter à la lecture de ce travail.

Et, du fond du cœur, merci à toute ma famille. A mon épouse, *informaticophobe*, pour les heures innombrables passées à relire et corriger ce texte, et à mes enfants pour tout le temps perdu à attendre que la place se libère derrière l'ordinateur familial. Merci pour avoir supporté cette vie entre parenthèses, pour votre patience, pour votre support, pour votre courage. Pour votre humour grinçant, aussi.

... et puis mon papa relit ce qu'il a écrit, et il n'y comprend plus rien. Alors il se dit: "et si je recommençais ?"

Nicolas, 12 ans.

Table des matières

Premier volume

TROISIEME PARTIE: Identification des menaces

CHAPITRE 6: Approche statistique

CHAPITRE 7: La méthode du CEA

CHAPITRE 8: La suite d'EBIOS

QUATRIEME PARTIE: LA TECHNOLOGIE

CHAPITRE 9: Notions de base

CHAPITRE 10: La voix sur IP

CHAPITRE 11: Identification et authentification

CHAPITRE 12: Chiffrement

CINQUIEME PARTIE: LE SYSTEME

CHAPITRE 13: Catalogue des exigences

CHAPITRE 14: Architecture

CHAPITRE 15: Mode d'acquisition

Second volume

Organisation du document

En tenant compte des annexes, ce document dépasse les 200 pages. Dans le but d'en faciliter les manipulations et la lecture, il a donc été scindé en deux volumes distincts.

Le premier volume contient le texte et tous les éléments essentiels de ce travail. Le second volume, quant à lui, reprend les éléments explicatifs ou illustratifs, à savoir le glossaire, les annexes et la bibliographie.

Conventions de notation

Marquage d'éléments

Chaque nouvel élément introduit auquel il pourrait être fait ultérieurement référence sera identifié par un identifiant écrit entre parenthèses et en caractères italiques, identifiant composé d'un nombre (identification du paragraphe) suivi d'une lettre (identification de l'élément dans le paragraphe). La plupart du temps le texte est autosuffisant et ces marqueurs peuvent être ignorés du lecteur; ils ne sont présents qu'à des fins de traçabilité.

Exemple dans le texte du paragraphe 2.1.1.:

... ce nouvel élément *(2.1.1.a)* dans le texte

Exemple dans une liste du paragraphe 2.1.3.:

- *(2.1.3.c)* nouvel élément de la liste introduisant éventuellement un nouvel élément *(2.1.3.d)* de texte

...

Renvoi à un élément marqué

Lorsqu'il est fait référence à un élément préalablement introduit et marqué, le code identifiant dudit élément est inséré en format exposant après la référence à l'élément en question.

Exemple:

... référence faite à un élément préalablement introduit [2.1.1.a] . . .

Renvoi à un autre paragraphe

Le renvoi explicite à un autre paragraphe se fait en insérant dans le texte le numéro du paragraphe en question. Toutefois, lorsqu'il est fait référence à un élément préalablement introduit mais non marqué spécifiquement, le numéro du paragraphe dans lequel l'élément a été introduit est inséré en format exposant après la référence à l'élément en question.

Exemples:

... comme en (4.1.2), la référence à cet élément préalablement introduit [2.3.5] nous incite à ...

Renvoi au glossaire

Certains termes sont parfois utilisés dans un sens bien défini qui fait alors l'objet d'une définition dans le glossaire. Il peut également arriver que cette signification prédéfinie diffère de l'acception traditionnelle du terme utilisé dans la langue française, acception traditionnelle à laquelle nous pouvons également avoir recours. Afin de lever toute ambiguïté sur ce plan, chaque fois qu'un terme ou une expression sera utilisé(e) dans un sens particulier tel que défini par le glossaire, ce terme ou cette expression sera suivi(e) d'un [G].

Lors de l'utilisation d'une abréviation, le renvoi au glossaire est automatique et implicite.

Exemple:

Si dans certains contextes - tel celui d'UML - l'utilisateur[G] est un concept qui revêt une signification particulière, il s'avère parfois inutile voire pénalisant d'appauvrir notre vocabulaire et d'user de périphrases pour ne pas parler d'un utilisateur dans le sens traditionnel du terme.

Renvoi à la bibliographie

Lorsqu'il est fait référence à un élément issu d'un ouvrage repris dans notre bibliographie, l'identifiant de cet ouvrage dans notre bibliographie sera repris entre crochets.

Exemples:

... établie par modélisation du protocole [Leduc-99], mais aussi ....
[Leduc-99] a démontré ...

La seule exception à cette règle concerne les RFC.

Mise en évidence

Lorsque nous souhaiterons attirer l'attention du lecteur sur un terme ou une expression, ou lorsque nous développerons un par un les éléments d'une liste énumérative, le terme ou expression (représentant éventuellement l'élément de la liste) sera écrit en *caractères italiques*.

Exemples:

... selon un schéma *dichotomique* simple:

- c'est vrai, ou
- c'est faux.

Si c'*est vrai*, alors ...

Notes infrapaginales

Les notes infrapaginales sont numérotées en continu sur l'ensemble du document; elles se présentent sous la forme d'un simple chiffre ou nombre[1] placé en exposant et renvoyant au bas de la même page.

[1] Exemple de note infrapaginale

Introduction

Objectifs et présentation

L'objet du présent document est l'*analyse de risques*[G] *dans le cadre de la mise en place d'une application distribuée sur l'Internet*. Basé sur un cas réel dans une entreprise existante, ce document ne constitue pas une démarche absolue mais plutôt un essai d'application à un exemple concret.

L'objectif poursuivi est donc pluriel. D'une part, nous souhaitons apporter à l'entreprise concernée une assistance à la décision de s'équiper ou non d'une telle application et, en cas de décision positive, lui fournir des indications utiles à l'établissement des spécifications initiales comme au choix de l'architecture et du mode d'acquisition du produit. Mais cette assistance et ces indications reposeront largement sur une étude de risques[G], qui constituera l'essentiel de ce travail, et visera à déterminer nos exigences en matière de sécurité pour la nouvelle application en tenant compte de l'environnement technique et organisationnel dans lequel elle est appelée à s'insérer.

Notre démarche, traditionnelle, consistera après la description du contexte de l'application à en préciser les *besoins de sécurité*[G]. Ceux-ci établis, nous nous attacherons à identifier les menaces[G] correspondantes puis, après un petit détour destiné à clarifier certains aspects technologiques, à établir une description fonctionnelle et technique de l'application projetée. Cette description servira in fine à l'établissement d'une liste de critères sur base desquels s'opèrera le choix du produit à acquérir, ou la décision de le développer.

La structure de ce document reflète la démarche résumée ci-dessus.

La première partie sera consacrée au contexte initial du projet: elle comportera une très brève présentation de l'entreprise, de l'origine du projet et de ses objectifs, ainsi qu'une première description de nos attentes fonctionnelles. Après l'expression des besoins de sécurité[G] (deuxième partie) et l'étude des menaces[G] (troisième partie), nous aborderons certains aspects plus techniques (quatrième partie) qui nous aideront à dessiner le produit recherché et à décider de son mode d'acquisition (cinquième partie).

Pour cette étude aucune méthode n'était imposée par l'entreprise; aucune ne nous était par ailleurs familière. Afin d'atteindre un niveau de confiance satisfaisant quant aux résultats escomptés mais aussi - pourquoi le taire - par curiosité, nous avons donc quelques fois tenté d'emprunter plusieurs itinéraires différents pour parvenir à nos fins. Le cas échéant, la première approche suivie aura toujours été une démarche personnelle, une expérimentation, suivie dans le texte comme dans le temps par l'utilisation d'une méthode documentée et plus structurée.

Première partie LE PROJET

Présentation du contexte général: l'entreprise, l'origine du projet, ses objectifs, et première définition fonctionnelle.

Chapitre 1 Contexte du projet

Présentation très rapide des éléments du contexte qui ont une influence significative sur le projet.

1.1. L'entreprise

1.1.1. Secteur d'activité

L'entreprise qui sert de cadre à ce projet est une petite société de services en informatique qui compte relativement peu d'employés - une petite dizaine seulement pour le siège central *(1.1.1.a)*. Cette entreprise développe et commercialise plusieurs logiciels de gestion administrative (logiciels 'ERP', comptabilité) ainsi que certains outils 'système' ou services de nature variée *(1.1.1.b)*.

Les évolutions récentes des technologies de l'information ayant conduit l'entreprise à redéfinir sa stratégie, elle tente pour le moment de se positionner comme acteur dans le marché de l'ASP, du commerce électronique[2] et de l'hébergement de serveurs HTTP *(1.1.1.c)*.

1.1.2. Distribution géographique

De par sa clientèle, constituée en bonne partie de grands comptes internationaux, mais aussi de par sa stratégie propre, l'entreprise s'est fortement distribuée géographiquement avec des filiales dans plusieurs pays d'Europe mais aussi aux USA et dans l'ancienne URSS *(1.1.2.a)*. Il n'est donc pas rare d'y trouver, collaborant à un même projet, un ou plusieurs employés de l'une ou l'autre implantation.

Outre cette distribution géographique en filiales, l'entreprise s'est encore davantage décentralisée par le développement des possibilités de télétravail *(1.1.2.b)* et la grande mobilité de certaines catégories de personnel *(1.1.2.c)*.

1.1.3. Disparité technologique

Parallèlement à sa dispersion géographique, l'entreprise se caractérise également par l'existence d'une grande disparité technologique *(1.1.3.a)* en partie due à un faible niveau de centralisation. Au niveau des systèmes d'exploitation, toutes les versions récentes de Windows coexistent avec au moins deux versions d'Unix et trois distributions de Linux (qui apparaît au niveau des postes de travail). Les dispositifs de protection logique des sites importants (pare-feu) ont été choisis et implémentés en toute indépendance par les responsables de chaque site, et il en va de même du mode de connexion des employés et filiales à l'Internet, allant du dialup 56kpbs (PSTN) jusqu'à la ligne louée en passant par l'ISDN et l'incontournable ADSL.

[2] Sites B2B uniquement, sans fonctionnalités de payement électronique.

1.2. Le projet

1.2.1. Description

Le projet qui servira de cadre à ce document consiste en la mise en place d'une application de communication vocale via l'Internet.

1.2.2. Origine

L'origine et les objectifs initiaux de ce projet sont la combinaison d'une démarche générale de réduction des coûts au sein de l'entreprise *(1.2.2.a)* et de la recherche d'une plus grande efficacité de la collaboration interne *(1.2.2.b)* comme du support client *(1.2.2.c)*.

1.2.3. Place du projet dans l'entreprise

Ce projet n'est pas stratégique, en ce sens qu'il ne fait pas partie des objectifs et du plan de développement stratégiques de l'entreprise [1.1.1.c] *(1.2.3.a)*. Il est considéré par la direction comme une idée intéressante, valant la peine qu'on y consacre un peu de temps quand il y en a et qui, s'il devait se concrétiser, serait testé et évalué avec intérêt; entre-temps, aucune autre ressource n'y sera officiellement affectée *(1.2.3.b)*. Notons toutefois que plusieurs employés, en fonction des besoins et des possibilités, utilisent déjà sporadiquement des outils comme NetMeeting (de MicroSoft) ou Groove (de Groove Networks) pour communiquer entre eux *(1.2.3.c)*.

Chapitre 2 Objectifs du projet

Présentation très rapide des objectifs qui sont à l'origine du projet.

2.1. Les objectifs Généraux

2.1.1. La maîtrise des coûts

Confrontée à une situation économique difficile, l'entreprise se voit contrainte de mieux maîtriser ses coûts (1.2.2.a) *(2.1.1.a)*, et parmi eux ses frais de télécommunication dont la croissance fut importante ces dernières années (décentralisation accrue (1.1.2.a) (1.1.2.b) (1.1.2.c), multiplication des téléphones mobiles et investissement stratégique dans une ligne louée vers l'Internet avec SLA(1.1.1.c)).

Cette maîtrise des coûts de l'entreprise emprunte plusieurs chemins dont deux, a priori antagonistes, nous intéressent particulièrement ici: la réduction des frais téléphoniques *(2.1.1.b)* et la diminution de la superficie de bureau occupée par l'intensification du recours à des formules de télétravail (1.1.2.b) *(2.1.1.c)*. D'autres possibilités de réduction de frais existent *(2.1.1.n)*, mais sortent du cadre de ce document.

2.1.2. La recherche de synergies

Dans le contexte économique auquel nous avons fait allusion ci-dessus, et tenant compte de la grande dispersion géographique (1.1.2.a) (1.1.2.b) (1.1.2.c) d'un personnel peu nombreux (1.1.1.a) par rapport au catalogue de produits et services disponibles (1.1.1.c) (1.1.1.b), le besoin d'outils facilitant la collaboration entre employés distants ne devient que plus important encore (1.2.2.b) *(2.1.2.a)*.

2.1.3. L'amélioration du support

La fonction de support des clients n'est pas plus centralisée que l'entreprise elle-même, et n'est guère facilitée par les caractéristiques de quantité et de dispersion du personnel comme de l'activité déjà évoquées ci-dessus. En pratique et la plupart du temps, le client qui rencontre une difficulté sait quels employés sont en mesure de lui prêter assistance, et il les contacte directement. Cette manière de procéder, toutefois, présente quelques inconvénients:

- faible professionnalisme: si une personne n'est pas joignable (en réunion, en congé, ...), c'est le client qui doit chercher un autre interlocuteur;
- faible évolutivité: cette façon de procéder ne sera plus tenable avec davantage de clients répartis sur plusieurs fuseaux horaires;
- coût élevé: nombreuses communications internationales à facturation partagée (téléphonie mobile).

En permettant aux clients de voir directement quels employés sont disponibles *(2.1.3.a)* et de les joindre via l'Internet, le système contribuera à améliorer la qualité du support de l'entreprise (1.2.2.c) *(2.1.3.b)*.

2.2. Les objectifs concrets

La direction choisie pour atteindre ces objectifs est celle de la mise en place d'outils de collaboration utilisant l'Internet comme support *(2.2.a)*; dans la suite de ce document, nous nous limiterons volontairement à l'aspect de communication vocale (2.1.1.b) *(2.2.b)*, les autres aspects et types d'outils étant simplement évoqués ici pour mémoire *(2.2.n)*.

2.3. Tableau et arborescence des objectifs

Une liste récapitulative (tableau 2.1) et un graphe d'arborescence (figure 2.1) résument les points précédents.

Tableau 2.1	**Liste des objectifs**		
Identifiant	*Libellé court*	*Libellé long*	*Contribue à*
(2.1.1.a)	réd. frais	Réduire les frais généraux	
(2.1.1.b)	frais tél.	Réduire les frais téléphoniques	(2.1.1.a)
(2.1.1.c)	frais loc.	Réduire la superficie de bureaux occupée	(2.1.1.a)
(2.1.1.n)	autres fr.	Autres stratégies de réduction de frais (pour mémoire)	(2.1.1.a)
(2.1.2.a)	synergie	Développer les synergies internes	
(2.1.3.b)	support	Améliorer la qualité du support	
(2.2.a)	outils	Mettre en place des outils de collaboration via l'Internet	(2.1.1.b) (2.1.1.c) (2.1.2.a) (2.1.3.b)
(2.2.b)	voix	Mettre en place des outils de communication vocale via l'Internet	(2.2.a)
(2.2.n)	autres ou.	Mettre en place d'autres outils de collaboration via l'Internet	(2.2.a)

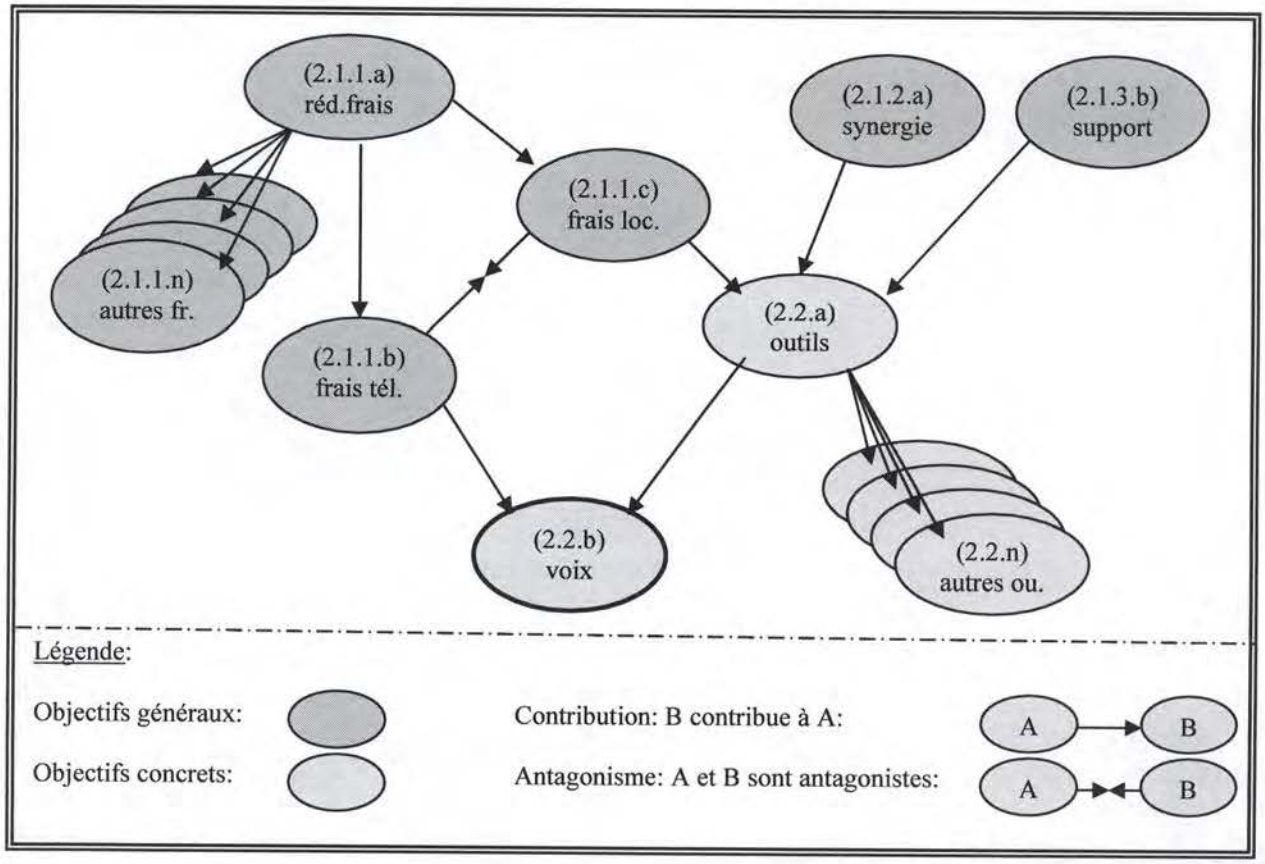


Figure 2.1: arborescence des objectifs

Chapitre 3 Esquisse fonctionnelle

Dans ce chapitre, nous décrirons très brièvement l'application du point de vue fonctionnel. L'objectif n'est pas d'en établir ici le cahier de charges, mais de préciser le point de départ de notre démarche.

3.1. Objectifs opérationnels

La finalité opérationnelle du système (2.2.b) consiste à permettre:

- *(3.1.a)* aux employés de l'entreprise de parler avec n'importe quel client (2.1.3.a) ou employé (2.1.2.a) de l'entreprise via l'Internet, et
- *(3.1.b)* aux clients de l'entreprise de parler avec n'importe quel employé de l'entreprise via l'Internet (2.1.3.a).

Ainsi énoncée, cette finalité nous permet d'avancer les restrictions suivantes:

- *(3.1.c)* le système n'est pas public, puisque seuls les clients et employés de l'entreprise y ont accès;
- *(3.1.d)* les clients de l'entreprise ne sont pas censés pouvoir utiliser le système pour converser entre eux.

A cet énoncé de base, l'objectif général de recherche de synergies (2.1.2.a) nous pousse à ajouter que le système devra pouvoir fonctionner en mode conférence (communication à plus de deux personnes) *(3.1.e)*, comme cela se pratique déjà aujourd'hui avec certains outils de collaboration que nous utilisons parfois (1.2.3.c).

3.2. Acteurs

Au stade actuel de notre démarche nous identifions trois types d'acteurs:

- *(3.2.a)* les clients de l'entreprise,
- *(3.2.b)* les employés de l'entreprise et
- *(3.2.c)* un acteur secondaire incontournable: un responsable administrateur du système.

3.3. Fonctions

3.3.1. Analogie téléphonique

L'analogie de notre projet par rapport à un système de téléphonie classique est évidente et sera exploitée ici pour nous aider à dégager aisément les principales fonctionnalités à considérer.

Pour fonctionner et être utilisable, un système de téléphonie classique (fixe ou mobile) doit remplir certaines conditions:

- il doit exister, c'est-à-dire avoir fait l'objet
  - *(3.3.1.a)* d'un développement et
  - *(3.3.1.b)* d'un déploiement;
- il doit comprendre un certain nombre d'éléments:
  - *(3.3.1.c)* des postes individuels,
  - *(3.3.1.d)* une infrastructure (matériels et logiciels) de communication et
  - *(3.3.1.e)* un répertoire ou index;
- il doit également offrir à l'utilisateur un certain nombre de fonctionnalités[3]:

[3] Cette liste de fonctionnalités n'a pas la prétention d'être universelle ni complète; elle n'est établie ici que comme base ou hypothèse de travail.

- *(3.3.1.f)* la possibilité de raccorder son poste individuel à une infrastructure de communication;
- *(3.3.1.g)* la possibilité de consulter le répertoire;
- *(3.3.1.h)* la possibilité de composer un numéro (invitation[G]);
- *(3.3.1.i)* la possibilité de mettre fin à une invitation[G];
- *(3.3.1.j)* la notification de l'invitation[G] au destinataire;
- *(3.3.1.k)* la possibilité de répondre à une invitation[G];
- *(3.3.1.l)* la possibilité de communiquer
- *(3.3.1.m)* la possibilité de mettre fin à une communication

Ce sont ces différentes fonctions qui nous intéressent ici, fonctions dont certaines sont illustrées par le diagramme de séquence de la figure 3.1.

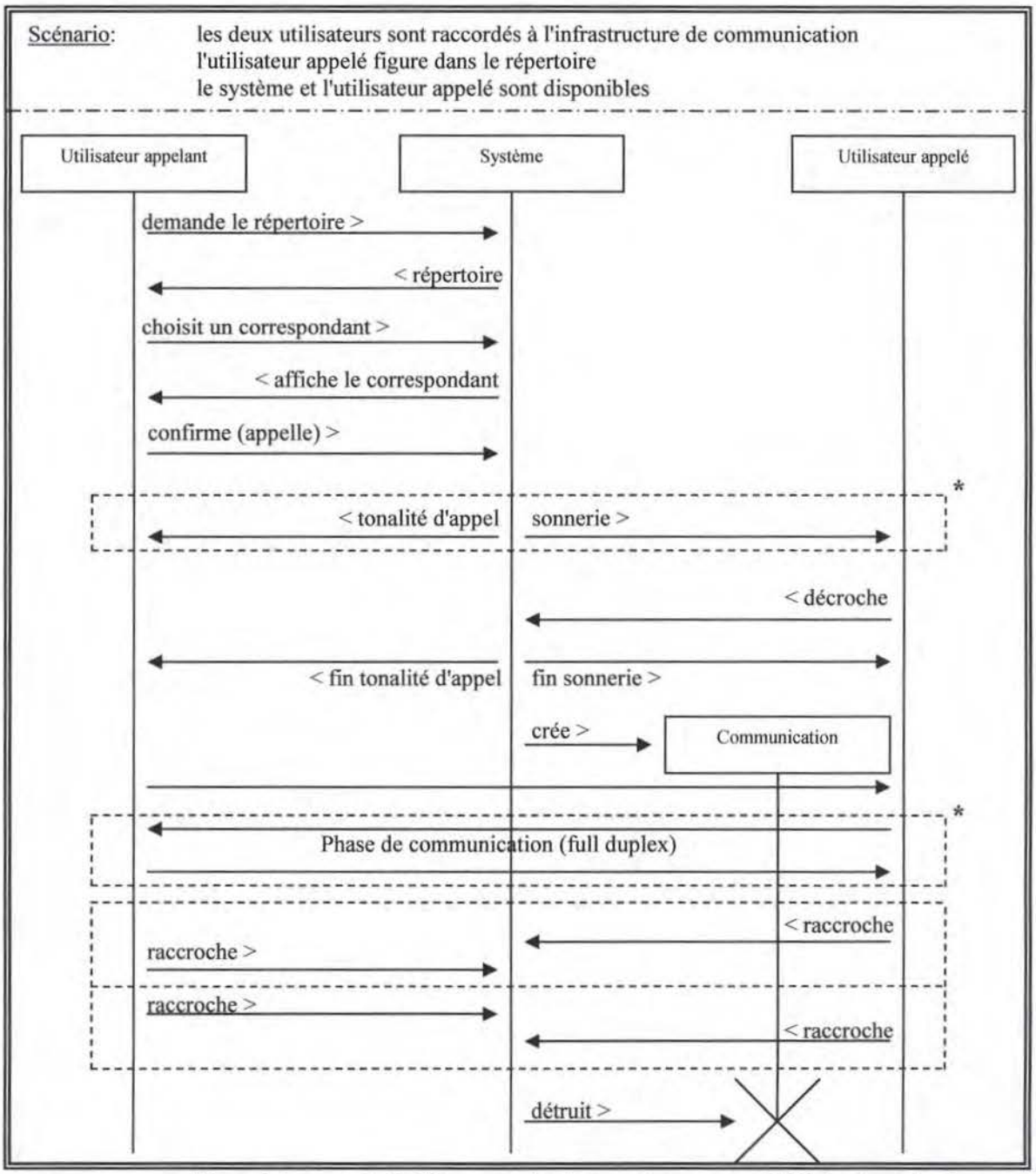


Figure 3.1: exemple de diagramme de séquence pour un appel téléphonique classique

3.3.2. Le raccordement à l'infrastructure de communication

En téléphonie classique (fixe ou mobile), le raccordement à l'infrastructure de communication est porteur d'informations dont celle qui nous concerne le plus est probablement celle qui permet à notre opérateur de nous identifier, c'est-à-dire dans la plupart des cas de nous facturer. Par rapport à notre application, cette fonctionnalité correspondra donc à la nécessaire identification[G] de l'utilisateur préalable à toute utilisation du système (3.1.c).

La logique élémentaire exige également, dès lors que nous envisageons une connexion[G] *(3.3.2.a)* au système, consécutive à l'identification de l'utilisateur[G], de prendre également en considération l'opération inverse de déconnexion *(3.3.2.b)*.

3.3.3. La consultation du répertoire

Notre répertoire (le "bottin" de notre application) devra logiquement afficher la liste de tous les utilisateurs raccordés à notre infrastructure au sens décrit en (3.3.2) (2.1.3.a). Il s'agira donc d'un répertoire assez dynamique, puisque le nombre de personnes qui s'y trouveront reprises variera au fil des connexions[G] (3.3.2.a) et déconnexions (3.3.2.b) des utilisateurs *(3.3.3.a)*.

De plus, la restriction qui consiste à ne pas permettre à nos clients d'exploiter le système pour communiquer entre eux (3.1.d) nous impose de rendre la gestion du répertoire plus intelligente, en choisissant:

- *(3.3.3.b)* soit de ne pas permettre l'invitation[G] quand l'invitant et l'invité sont des clients,
- *(3.3.3.c)* soit de ne pas permettre aux clients de voir les autres clients dans le répertoire.

Politiquement, la seconde solution nous semble plus correcte.

3.3.4. L'invitation

Après avoir sélectionné son correspondant grâce au répertoire[4], l'utilisateur déclenchera l'invitation[G] en confirmant son choix *(3.3.4.a)*. Cette procédure d'invitation[G] sera terminée par un des trois événements suivants:

- *(3.3.4.b)* soit l'invitant renonce - il devra donc être en mesure d'abandonner la procédure d'appel et de revenir au répertoire,
- *(3.3.4.c)* soit l'invité répond ('décroche') et la communication peut commencer,
- *(3.3.4.d)* soit l'invitation[G] est annulée par l'expiration d'un temporisateur avant qu'un des deux événements qui précèdent n'ait lieu, et l'invitant se retrouve au niveau de son répertoire..

Pendant toute la durée de l'invitation[G], une notification de l'invitation[G] doit parvenir à l'invitant comme à l'invité par au moins une des deux méthodes suivantes:

- *(3.3.4.e)* via un signal sonore (sonnerie) ou
- *(3.3.4.f)* via un signal visuel ('pop up').

Si l'invité décroche, la communication commence (3.3.4.c). Dans tous les autres cas (3.3.4.b) (3.3.4.d) l'invité devra être informé de la tentative d'invitation[G], des date et heure à laquelle elle s'est produite et de son origine *(3.3.4.g)*.

3.3.5. La communication

La communication vocale entre l'invitant et l'invité sera une communication en duplex intégral. Au cours de cette communication, tant l'invitant que l'invité pourront effectuer une des deux actions suivantes:

[4] En pratique, l'utilisateur pourrait introduire directement les premières lettres du nom de son correspondant: c'est alors le système lui-même qui consulterait le répertoire et effectuerait, le cas échéant, la sélection du correspondant recherché.

- *(3.3.5.a)* mettre fin à la communication, ou
- *(3.3.5.b)* décider d'inviter un autre utilisateur - en retournant au répertoire - afin qu'il se joigne à la communication en cours (mode *conférence* (3.1.e)), avec pour l'invitant retour à la communication en cours en cas de succès (3.3.4.c) comme en cas d'échec (3.3.4.b) (3.3.4.d) *(3.3.5.c)* de l'invitation[G].

3.3.6. L'administration du système

Paraphrasant l'adage populaire qui affirme qu'il n'y a pas d'horloge sans horloger, nous dirions ici qu'il n'est pas davantage de système sans administrateur. Ses responsabilités seront de deux ordres:

- *(3.3.6.a)* permettre l'enrôlement[G] des utilisateurs (à même titre que celui qui vous vend un contrat de téléphonie mobile enregistre vos données personnelles), et
- *(3.3.6.b)* garantir la continuité du service.

3.4. Diagramme

3.4.1. Diagramme d'états de l'utilisateur

La figure 3.2 ci-dessous récapitule les différents états de l'utilisateur de notre système.

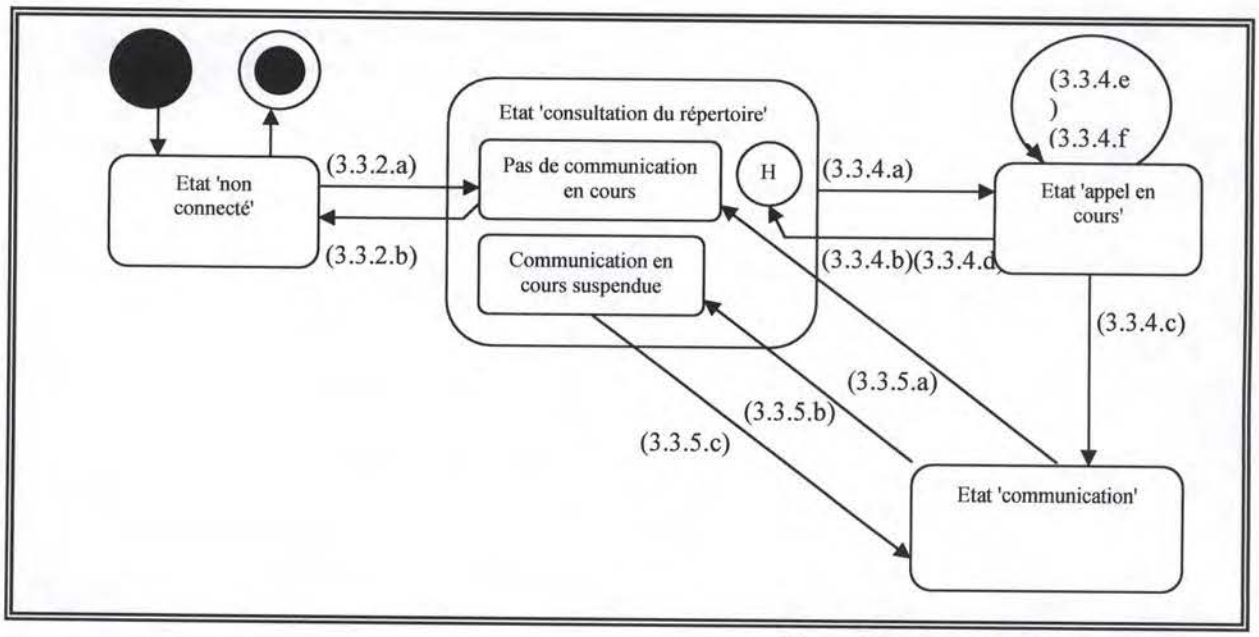


Figure 3.2: états de l'utilisateur enrôlé

Deuxième partie: Expression des besoins de sécurité

Identification de nos besoins de sécurité, ou le genre de conséquence que nous ne pouvons pas nous permettre. Ces besoins sont fonction de l'entreprise, du type d'activité et du profil du projet.

Chapitre 4 Réflexion fondamentale

Réflexion fondamentale, ou tentative de détermination de nos besoins de sécurité en suivant une démarche personnelle que nous pourrions qualifier d'intuitive.

4.1. Introduction

Le contexte spécifique du déploiement d'une application distribuée dans un environnement existant nous pousse à déterminer nos besoins de sécurité selon deux points de vue:

- le point de vue de la sécurité intrinsèque de la nouvelle application, et
- celui de l'impact de la nouvelle application sur la sécurité de l'ensemble préexistant.

Pour y arriver, nous procéderons comme suit:

- nous définirons les objets de la sécurité, ou ce que nous cherchons à protéger;
- nous définirons un certain nombre de critères de la sécurité;
- nous définirons une échelle d'évaluation de l'impact d'un sinistre;
- pour chaque critère d'évaluation défini, nous évaluerons:
  - la pertinence de ce critère,
  - l'impact sur nos objets (et donc pour l'entreprise) d'un sinistre par rapport à ce critère et,
  - si impact significatif il pourrait y avoir, nous envisagerons quelques possibilités d'exigences que nous pourrions poser sur l'application pour éviter que cela se produise.

4.2. Objets et critères de la sécurité

Les objets de la sécurité représentent ce que nous cherchons réellement à préserver, et dans le cadre de cette étude nous en identifions trois principaux:

- *(4.2.a)* les objectifs généraux du projet (2.1.1.a) (2.1.2.a) (2.1.3.b),
- *(4.2.b)* l'image de marque de l'entreprise et
- *(4.2.c)* l'entreprise elle-même, par une atteinte à ses objectifs stratégiques (1.1.1.c).

Notre liste de critères pour évaluer la sécurité de l'application est constituée de cinq propriétés fondamentales dont l'absence nous paraît être de nature à porter atteinte aux objets précités. Sans beaucoup de surprise, les propriétés en question sont:

- la disponibilité[G],
- la confidentialité[G],
- l'imputabilité[G],
- l'écologie[G] et
- l'intégrité[G]

Enfin, pour évaluer l'impact potentiel d'un sinistre, nous utiliserons une échelle simple à quatre niveaux largement inspirée des travaux du Comité Européen des Assurances [CEA]:

- niveau 0: *non significatif*; aucun impact, ou impact marginal
- niveau 1: *significatif*; nécessiterait un effort réel (financier ou autre) pour l'assumer
- niveau 2: *grave*: un sinistre pourrait pousser l'entreprise à reconsidérer son (ses) objectif(s)
- niveau 3: *catastrophique*: un sinistre mettrait en cause la pérennité de l'entreprise

L'évaluation du niveau de l'impact sur les objets à protéger d'un sinistre potentiel affectant une ou plusieurs des propriétés fondamentales d'une application, et ceci dans le contexte d'une entreprise particulière, est un exercice délicat comprenant une très grande part de subjectivité liée principalement à notre perception du contexte général de l'entreprise. Nous essayerons donc, le plus souvent possible, de motiver notre perception des choses.

4.3. Disponibilité de l'application

4.3.1. Pertinence du critère

En quelques mots, nous pouvons considérer qu'il y a atteinte à la disponibilité[G] du système lorsqu'une ou plusieurs des situations suivantes se présente(nt):

- *(4.3.1.a)* si le système ne fonctionne pas, quelle qu'en soit la cause (interne ou externe) ;
- *(4.3.1.b)* si le système fonctionne mais que tous les utilisateurs[G] habilités n'y ont pas accès;
- *(4.3.1.c)* si le système fonctionne, que les utilisateurs[G] habilités y ont accès mais que certains n'y trouvent pas le correspondant recherché (cas du client qui cherche du support quand aucun employé n'est connecté (2.1.3.a));
- *(4.3.1.d)* si le niveau des performances réelles du système décourage son utilisation.

4.3.2. Evaluation de l'impact

Par rapport aux objectifs de maîtrise des coûts (2.1.1.a) et de recherche de synergies (2.1.2.a), l'application n'est pas critique (1.2.3.a) (une alternative simple consiste à travailler comme actuellement: téléphone, mail, fax, Groove (1.2.3.c)). Un incident / accident rendant l'application *provisoirement* indisponible ne représente pas a priori une menace[G] importante *(4.3.2.a)*. Par rapport à l'objectif d'amélioration du support (2.1.3.b) l'approche est différente: si l'application devait être mise en service et exploitée dans ce sens, sa disponibilité[G] deviendrait alors un élément à prendre en considération *(4.3.2.b)*. Et en ce qui concerne l'image de l'entreprise, il vaut probablement mieux ne pas proposer d'utiliser un système à un client qui n'en exprime pas la demande que de lui en proposer un qui ne lui donnerait pas satisfaction (mécontentement du client, ternissement de l'image de marque du fournisseur) *(4.3.2.c)*.

Enfin, par rapport aux objectifs stratégiques de l'entreprise (1.1.1.c), le manque de disponibilité[G] d'une application non stratégique (1.2.3.a) ne devrait pas porter à conséquence *(4.3.2.d)*.

Tableau 4.1. Evaluation de l'impact d'un problème de disponibilité

Cible potentielle	*Impact*	*Motivation principale*
Objectif de réduction des coûts (2.1.1.a)	0	(4.3.2.a)
Objectif de recherche de synergies (2.1.2.a)	0	(4.3.2.a)
Objectif d'amélioration du support (2.1.3.b)	1	(4.3.2.b)
Image de l'entreprise (4.2.b)	1	(4.3.2.c)
Objectifs stratégiques de l'entreprise (1.1.1.c)	0	(4.3.2.d)

4.3.3. Mesures proposées

Le problème de la disponibilité[G] comporte des aspects quantitatifs et qualitatifs.

Quantitativement, ils peuvent s'exprimer sous la forme du nom respect d'un SLA de base qui pourrait être par exemple défini comme suit:

- le système est destiné à être exploité pendant les heures de bureau et jours ouvrables de l'entreprise et de ses clients (concept de *journée de support*);
- les heures de bureau actuelles sont 08H00 AM (GMT +3) à 06H00 PM (GMT -5), soit de 06H00 AM à 12H00 PM heure belge;
- *(4.3.3.a)* les heures de bureau pourraient s'étendre davantage (23/24) en cas de succès de certains contacts entrepris en Malaisie (GMT +8);
- un jour est considéré comme jour ouvrable si il l'est pour au moins un des clients de l'entreprise;
- le concept *d'inaccessibilité du système* est défini comme suit:
  - il y a inaccessibilité du système quand, pendant une journée de support, un client ne parvient pas à se connecter au système (4.3.1.a)(4.3.1.b) ou que, connecté, il n'y trouve aucun agent du support (employé) (4.3.1.c);
  - le fait que le système atteigne sa capacité nominale (toutes les 'lignes' occupées), ou que tous les agents du support (employés) soient occupés, n'est pas considéré comme une inaccessibilité du système
- il y a *interruption de service* en cas d'inaccessibilité du système non imputable à des éléments hors de notre contrôle (accidents physiques d'origine externe, force majeure, perte de services essentiels, grève);
- il y a *continuité de service* si on compte moins de 30 minutes d'interruption de service sur une journée de support
- il y a *discontinuité de service mineure* si on compte entre 31 et 60 minutes d'interruption de service sur une journée de support
- il y a *discontinuité de service majeure* si on compte entre 61 et 120 minutes d'interruption de service sur une journée de support
- il y a *discontinuité de service totale* si on compte plus de 120 minutes d'interruption de service par journée de support
- l'entreprise s'engage sur base du SLA suivant:
  - au maximum une discontinuité de service totale par an
  - au maximum une discontinuité de service majeure par mois
  - au maximum une discontinuité de service mineure par semaine

Ce SLA semble peu contraignant mais concrètement, le garantir (donc garantir la disponibilité[G] telle qu'elle y est définie) consiste à prendre les mesures suivantes:

- *(4.3.3.b)* avoir tous les jours de la semaine une personne compétente apte à intervenir et à résoudre un problème impliquant une interruption de service, et ce en moins de 2 heures, déplacement éventuel compris (4.3.1.a). On peut se demander si le coût d'une telle mesure de protection n'est pas disproportionné par rapport à l'impact estimé en 4.3.2. De plus, cette obligation est davantage une mesure organisationnelle qui sort du cadre de ce document;
- *(4.3.3.c)* avoir en permanence tout au long de la journée de support au moins un employé connecté au système (4.3.1.c) . Cette obligation constitue, par ailleurs, une mesure organisationnelle qui sort également du cadre de ce document;
- *(4.3.3.d)* avoir en permanence tout au long de la journée de support une partie des ressources du système réservée aux appels des clients;
- *(4.3.3.e)* faire en sorte que l'accès et l'utilisation du système soient possibles pour toute personne autorisée, quel que soit son lieu de travail (1.1.2.a)(1.1.2.b)(1.1.2.c), son type de poste de travail (1.1.3.a) et son mode de connexion à l'Internet (1.1.3.a).

Qualitativement, nous avons considéré qu'il y avait manque de disponibilité[G] lorsque les performances réelles ne permettent plus à deux personnes d'entretenir une conversation normale (4.3.1.d). Ces mauvaises

performances[5] peuvent être conjoncturelles (passagères: fonction de la 'météorologie' de l'Internet) ou structurelles (persistantes: intrinsèques au système, qui ne permettrait pas par exemple de définir un nombre maximum de communications simultanées) *(4.3.3.f)*. En règle générale, il vaudra mieux que le système refuse l'établissement d'une communication supplémentaire plutôt que de l'accepter en dégradant fortement toutes les communications en cours (caractéristique du streaming[G], non élastique). Deux cas de figure sont donc à envisager:

- *(4.3.3.g)* si le système est destiné à être exploité dans un contexte où une bande passante et des garanties de service (délais et variabilité du délai) lui sont offertes, alors il devra disposer d'un paramètre de configuration permettant d'adapter le nombre maximum de communications aux garanties en question (4.3.3.d);
- *(4.3.3.h)* dans le cas contraire le système devra au minimum disposer d'un mécanisme de mesure des performances du réseau ou de la qualité des communications en cours, et autoriser ou non l'établissement d'une communication supplémentaire en fonction du résultat de ces mesures. De plus, les performances des réseaux étant parfois assez fluctuantes, la mesure précédente (4.3.3.g) permettrait de limiter davantage les risques en fixant un plafond.

4.4. Confidentialité de l'application

4.4.1. Pertinence du critère

Le critère de confidentialité[G] peut être envisagé à plusieurs niveaux:

- la confidentialité[G] de l'application elle-même:
  - *(4.4.1.a)* son existence en tant que projet;
  - *(4.4.1.b)* son existence en tant qu'application exploitée par l'entreprise;
- *(4.4.1.c)* la confidentialité[G] du code source de l'application;
- la confidentialité[G] des données de l'application:
  - confidentialité[G] des données persistantes:
    - *(4.4.1.d)* paramètres de connexion[G] (identifiant et mot de passe, par exemple) (3.3.2.a) et
    - *(4.4.1.e)* profils utilisateurs (attributs divers de l'utilisateur) (3.3.6.a);
  - confidentialité [G] des données non persistantes:
    - *(4.4.1.f)* le contenu des conversations et
    - *(4.4.1.g)* l'identité des participants à une conversation;
- *(4.4.1.h)* la confidentialité[G] des protocoles (échanges) de l'application.

4.4.2. Evaluation de l'impact

La confidentialité[G] du *projet d'application* (4.4.1.a) peut revêtir une certaine importance dans la mesure où la vulnérabilité d'une application est habituellement plus élevée au cours des phases de développement et d'implémentation. Toutefois, un manque de confidentialité[G] au cours de ces phases ne devrait avoir aucun impact direct *(4.4.2.a)*; seul un impact indirect serait à craindre si la perte de confidentialité[G] ouvrait la porte à une atteinte à un des autres critères, comme par exemple l'intégrité[G] du code. La confidentialité[G] (le secret) au sujet de l'*existence d'une telle application* en production (4.4.1.b) paraît quant à elle difficile à conserver et, a priori, assez peu utile *(4.4.2.b)*.

Les besoins de confidentialité[G] *du code source* (4.4.1.c) sont difficile à préciser ici puisqu'ils dépendront en grande mesure du caractère commercial et du mode d'acquisition de l'application: produit développé puis commercialisé par l'entreprise, produit tierce partie au code source non disponible, licence de type GNU Open Source, etc. Toutefois, dans tous les cas, l'éventuelle divulgation du code ne semble pas un élément de nature à avoir un impact significatif sur les objets de la sécurité (4.2.a) (4.2.b) (4.2.c) *(4.4.2.c)*.

[5] Nous n'abordons ici que la cause la plus probable de mauvaises performances, à savoir les performances du réseau (bande passante, délais et variations des délais), au détriment des incidents de type attaque *DoS*[G] ou erreur d'implémentation (non respect des objectifs (3.1.c) (3.1.d)).

Pour ce qui est des *données persistantes*, une atteinte à la confidentialité[G] des profils utilisateurs (4.4.1.e) nous poserait un problème important d'ordre déontologique, l'identité des différents utilisateurs - entendez des différents clients - ne pouvant normalement être divulguée sans l'assentiment de ceux-ci *(4.4.2.d)*.

L'impact d'un problème de confidentialité[G] au niveau des *paramètres de connexion*[G] (4.4.1.d) sera traité ultérieurement.

En ce qui concerne les *données non persistantes*, si le *contenu des conversations* (4.4.1.f) entre employés (développeurs des applications stratégiques) devait être dévoilé, cela pourrait poser un problème d'image mais risquerait surtout de compromettre les objectifs stratégiques de l'entreprise *(4.4.2.e)*. De même, un client qui aurait besoin de faire fréquemment appel au support n'aimera probablement pas que d'autres clients l'apprennent (4.4.1.g) (il préfèrera donc, le cas échéant, ne pas utiliser le système ce qui contreviendrait à l'objectif d'amélioration du support (2.1.3.a)) *(4.4.2.f)*; enfin, si deux cadres de l'entreprise entretenaient de fréquentes conversations au vu et au su de tous, ils ne pourraient probablement cacher longtemps l'existence d'un projet qu'ils auraient préféré ne pas devoir révéler déjà *(4.4.2.g)*.

Reste à envisager le problème de confidentialité[G] des *protocoles de l'application* (4.4.1.h). A ce stade tout ce que nous pouvons affirmer c'est que ces protocoles, quels qu'ils soient, transporteront des informations:

- *(4.4.2.h)* les protocoles d'enregistrement, d'identification[G] et d'authentification[G] des utilisateurs véhiculeront principalement les données persistantes (profils (4.4.1.e) et paramètres de connexion[G] (4.4.1.d) des utilisateurs), avec les conséquences envisagées plus haut (4.4.2.d);
- *(4.4.2.i)* les protocoles de communication véhiculeront principalement les données non persistantes (contenu des conversations, identité des participants à une conversation), ce qui au niveau des conséquences nous ramène également ci-dessus (4.4.2.e) (4.4.2.f) (4.4.2.g).

Tableau 4.2.	**Evaluation de l'impact d'un problème de confidentialité**	
Cible potentielle	*Impact*	*Motivation principale*
Objectif de réduction des coûts (2.1.1.a)	1	(4.4.2.g)
Objectif de recherche de synergies (2.1.2.a)	1	(4.4.2.g)
Objectif d'amélioration du support (2.1.3.b)	1	(4.4.2.f)
Image de l'entreprise (4.2.b)	1	(4.4.2.d)
Objectifs stratégiques de l'entreprise (1.1.1.c)	2	(4.4.2.e)

4.4.3. Mesures proposées

Les problèmes liés à une perte de confidentialité[G] méritent incontestablement toute notre attention; pour nous en protéger, les quelques mesures qui suivent nous paraissent représenter un jeu minimal:

- *(4.4.3.a)* le système offrira à chaque utilisateur client de l'entreprise une visibilité des autres utilisateurs qui sera réduite à la seule catégorie des employés de l'entreprise (4.4.2.d);
- *(4.4.3.b)* l'identité des participants à une conversation ne doit pas être visible (4.4.2.f) (4.4.2.g) par les personnes extérieures à cette conversation;
- *(4.4.3.c)* l'identité des participants à une conversation doit être connue (4.4.2.e) de tous les participants à cette conversation;
- *(4.4.3.d)* à l'exception des seules informations strictement nécessaires au bon fonctionnement du répertoire (voir 3.3.3 et 3.3.4), aucune donnée persistante (4.4.2.h) ne pourra transiter par le réseau public;
- *(4.4.3.e)* aucune donnée persistante (4.4.2.h) ne pourra être conservée sur une machine autre que le serveur de l'application;
- *(4.4.3.f)* le serveur de l'application (4.4.3.e) sera physiquement situé au siège central de l'entreprise;
- *(4.4.3.g)* l'enrôlement[G] et la gestion des utilisateurs seront confiés à un employé de l'entreprise qui sera nommé responsable du système (3.3.6.a) (4.4.3.d);
- *(4.4.3.h)* les communications devront rester inintelligibles pour toute personne qui les capterait (inévitable dans les réseaux de type broadcast[G] ou de type interconnecté) mais n'y participerait pas (4.4.2.e);
- *(4.4.3.i)* les échanges protocolaires du système devront rester inintelligibles pour toute personne qui les capterait mais ne serait pas directement concernée (4.4.2.h) (4.4.2.i);

- *(4.4.3.j)* les données persistantes (4.4.1.d) (4.4.1.e) échangées dans le cadre du fonctionnement du répertoire (4.4.3.d) devront rester inintelligibles pour toute personne qui les capterait mais ne serait pas directement concernée;

4.5. Imputabilité de l'application

4.5.1. Pertinence du critère

L'imputabilité[G] est une propriété qui combine trois exigences: connaître l'identité de l'utilisateur (le *qui*), savoir quelle action il a entreprise (le *quoi*), et à quel moment il l'a entreprise (le *quand*). Ces trois exigences sont incontournables dès lors qu'on souhaite, même dans un système non critique ou stratégique, faire appel à une fonction d'audit, ce qui n'est envisagé ici que d'une manière très limitée par exemple pour répondre à l'exigence fonctionnelle de notification (3.3.4.g). En effet, l'audit systématique de l'activité du système s'avérerait contradictoire par rapport à certaines de nos exigences de confidentialité[G] (4.4.2.g) *(4.5.1.a)*.

La propriété d'imputabilité[G] de l'application pourrait être altérée par plusieurs facteurs dont les plus importants nous paraissent être les suivants:

- *(4.5.1.b)* un problème au niveau de la conception (utilité[G]) ou de l'implémentation (conformité[G]) des routines ad hoc du système,
- *(4.5.1.c)* un problème au niveau de l'exécution des routines ad hoc du système (problèmes de ressources, attaque logique, etc.),
- *(4.5.1.d)* un problème d'atteinte à l'intégrité[G] des informations générées par les routines ad hoc du système ou
- *(4.5.1.e)* un problème de correction[G] ou d'atteinte à l'intégrité[G] des informations utilisées par les routines ad hoc du système.

Tenant compte du faible niveau d'audit demandé (4.5.1.a) qui se résume au cas particulier de la notification d'invitation[G] (3.3.4.g), c'est-à-dire à peu de routines produisant peu d'informations, il nous semble percevoir que la cause principale d'un problème d'imputabilité[G] serait, dans le cadre de notre application, à chercher du côté des informations utilisées (4.5.1.e). Ce qui, concrètement, nous amène à ne considérer la plupart du temps que la première des trois exigences évoquées au début de ce paragraphe: la question très générale du *qui*.

Il serait erroné de penser que cette question du *qui* ne se pose pas vraiment sous prétexte que les utilisateurs potentiels se connaissent personnellement, puisqu'avec le développement possible des activités (4.3.3.a) et tenant compte de la distribution géographique de l'entreprise (1.1.2.a) cette situation n'est pas destinée à durer indéfiniment. De plus, l'objectif d'amélioration du support comprend la nécessité, pour le client, d'être en mesure de visualiser d'emblée les employés accessibles via le système (2.1.3.a), ce qui suppose qu'au minimum chaque employé connecté au système ait été préalablement identifié d'une manière ou d'une autre. De leur côté, les employés devront savoir avec certitude à quel client ils ont affaire.

Pour qu'il en soit ainsi, trois conditions doivent être réunies:

- le système doit posséder un minimum d'informations concernant ses utilisateurs, et ce en vue de pouvoir les reconnaître (phase d'enrôlement[G]);
- chaque utilisateur du système doit décliner son identité lors de chacune de ses connexions[G] au système (phase d'identification[G]);
- le système doit vérifier si l'identité déclinée est authentique (phase d'authentification[G]).

Le problème auquel nous devons faire face ici est celui de l'usurpation d'identité *(4.5.1.f)*, laquelle peut se produire à différents stades et de différentes manières:

- *(4.5.1.g)* par compromission (divulgation, modification) du mot de passe de l'utilisateur (par exemple comme conséquence du problème de confidentialité[G] des paramètres de connexion[G] que nous avions éludé en 4.4.2);
- *(4.5.1.h)* en rejouant une séquence d'identification[G] et d'authentification[G];
- *(4.5.1.i)* en cas de mauvaise déconnexion ou de non déconnexion (absence de l'utilisateur);
- *(4.5.1.j)* par le vol d'une connexion[G] (attaque du style *man in the middle*[G]);

- *(4.5.1.k)* par usurpation d'identité lors de l'enrôlement[G];

4.5.2. Evaluation de l'impact

Le principe de l'identification au sens large étant acquis, les principales conséquences d'une situation dans laquelle une personne usurperait l'identité d'un (autre) utilisateur sont les suivantes:

- *(4.5.2.a)* risque de perte en disponibilité[G] pour l'utilisateur dont l'identité aura été usurpée (4.5.1.f), voire pour tous les utilisateurs clients si l'identité usurpée est celle de l'employé assurant le support (4.3.1.c);
- *(4.5.2.b)* risque de perte en disponibilité[G] en cas d'utilisation abusive à l'encontre d'un autre utilisateur (*DoS*[G]);
- *(4.5.2.c)* risque de perte en confidentialité[G], par exemple en cas d'usurpation de l'identité d'un employé par un non employé, ce qui permettrait à ce dernier de consulter la liste des clients utilisant le système (4.4.2.d);
- *(4.5.2.d)* risque de submergement des ressources de l'entreprise par la multiplication des demandes de support pour des incidents fictifs (*DoS*[G]);

Pour terminer, signalons encore que les possibilités d'erreurs dans la fonction de notification d'invitation[G] (3.3.4.g) pourraient, outre la confusion qu'elles génèreraient, s'avérer préjudiciables à l'objectif de recherche de synergies (2.1.2.a) *(4.5.2.e)* mais aussi et surtout à celui d'amélioration du support (2.1.3.b) *(4.5.2.f)*.

Tableau 4.3.	**Evaluation de l'impact d'un problème d'imputabilité**	
Cible potentielle	*Impact*	*Motivation principale*
Objectif de réduction des coûts (2.1.1.a)	0	
Objectif de recherche de synergies (2.1.2.a)	1	(4.5.2.b) (4.5.2.e)
Objectif d'amélioration du support (2.1.3.b)	2	(4.5.2.a) (4.5.2.b) (4.5.2.d) (4.5.2.f)
Image de l'entreprise (4.2.b)	1	(4.5.2.c)
Objectifs stratégiques de l'entreprise (1.1.1.c)	1	(4.5.2.d)

4.5.3. Mesures proposées

La plupart des mesures proposées concernent l'identification (au sens large) de l'utilisateur, et non celle du poste de travail (1.1.2.b) (1.1.2.c) *(4.5.3.a)*. Dans ce domaine, la meilleure sécurité est atteinte lorsque cette identification est réalisée sur base des trois piliers traditionnels qui sont:

- *(4.5.3.b)* identification[G] et authentification[G] par la reconnaissance d'un élément que l'utilisateur connait (login et mot de passe);
- *(4.5.3.c)* identification[G] et/ou authentification[G] par la reconnaissance d'un élément que l'utilisateur possède (par exemple, une carte à puce);
- *(4.5.3.d)* identification[G] et/ou authentification[G] par la reconnaissance d'un élément propre à l'utilisateur (domaine des techniques biométriques)

L'absence de ressources financières allouées à ce projet (1.2.3.b) ne nous permet probablement pas d'envisager a priori autre chose que l'utilisation du couple classique login et mot de passe (4.5.3.b), sous réserve de l'évaluation d'une autre technique d'authentification[G] purement logicielle de l'utilisateur basée sur les caractéristiques biométriques de sa frappe du clavier [Philippe-02]. Pour être finalement adoptée, cette technique devra prouver son efficacité dans un contexte où l'utilisateur, mobile, n'est pas davantage lié à un poste de travail (donc à un type de clavier) (4.5.3.a) que ne le sont ses paramètres de connexion[G] (4.4.3.e) (login, mot de passe, signature biométrique) *(4.5.3.e)*.

Au vu de ces éléments et tenant compte de ce qui a déjà été proposé auparavant (4.4.3.d) (4.4.3.e) (4.4.3.g) (4.4.3.h) (4.4.3.i), nous proposons le jeu de mesures suivant:

- *(4.5.3.f)* tout utilisateur qui souhaitera utiliser le système, que ce soit pour joindre d'autres utilisateurs ou être joint par eux, devra au préalable s'identifier par un login (4.5.3.b) et être authentifié par son mot de passe (4.5.3.b) et sa signature biométrique de frappe au clavier (4.5.3.d);

- *(4.5.3.g)* les séquences d'identification[G] et d'authentification[G] (4.5.3.f) telles qu'elles peuvent être captées par un observateur sur le réseau doivent lui être inintelligibles (4.4.3.i) (4.5.1.g);
- *(4.5.3.h)* les séquences d'identification[G] et d'authentification[G] (4.5.3.f) telles qu'elles peuvent être captées par un observateur sur le réseau ne pourront pas être rejouées (4.5.1.h);
- *(4.5.3.i)* l'identification[G] et l'authentification[G] d'un utilisateur devront être revalidées au minimum au début de chaque communication (4.5.1.i);
- *(4.5.3.j)* il ne doit pas être possible à une tierce personne présente sur le réseau d'usurper l'identité d'un utilisateur identifié et authentifié (4.5.1.j) (4.5.1.k);
- *(4.5.3.k)* l'employé de l'entreprise qui aura l'enregistrement des utilisateurs dans ses attributions (4.4.3.g) sera responsable de la validité (ce qui inclut la confidentialité[G] (4.4.1.d)) des données utilisateurs (principalement celles relatives à l'identité, l'identification[G] et l'authentification[G] (4.4.3.g)) qui lui seront soumises pour enrôlement[G] dans le système;
- *(4.5.3.l)* lorsqu'une trace de l'activité du système et/ou de ses utilisateurs [G] devra être générée, cette trace ne sera conservée que le temps strictement nécessaire et les informations qu'elle contiendra ne pourront être accessibles que par le (ou les) utilisateur(s)[G] à l'intention duquel (desquels) elle aura été générée (4.5.1.a);
- *(4.5.3.m)* les tentatives infructueuses d'authentification[G] devront être journalisées.

4.6. Ecologie de l'application

4.6.1. Pertinence du critère

Parallèlement à l'étude des principaux risques[G] qui pourraient porter atteinte à une des qualités intrinsèques de l'application projetée, il nous a semblé indispensable de prendre du recul par rapport à cette approche *application-centrique* et de nous poser la question de l'impact qu'elle-même pourrait avoir sur son environnement.

D'après le dictionnaire Petit Robert, l'écologie (E) est *l'étude des milieux où vivent les êtres vivants ainsi que des rapports de ces êtres entre eux et avec le milieu.* Par analogie, si nous acceptons l'hypothèse de base qui consiste à assimiler notre application à un *être vivant* dans un *milieu* qui serait son environnement informatique, cette définition nous pousse à envisager nos besoins en matière de sécurité en tenant compte de trois nouveaux éléments:

- *(4.6.1.a)* l'environnement informatique de notre application
- *(4.6.1.b)* les rapports entre notre application et les autres applications de son environnement
- *(4.6.1.c)* les rapports entre notre application et son environnement informatique

Les conséquences d'un impact de l'environnement ou des autres applications sur notre application étant habituellement prises en compte par l'analyse des atteintes aux autres critères d'évaluation de la sécurité de notre application, nous définirons donc l'écologie[G] comme la propriété d'une application qui, en fonctionnement nominal, ne porte pas atteinte à un quelconque des critères d'évaluation de la sécurité des applications voisines.

Cette nouvelle approche présuppose:

- *(4.6.1.d)* la connaissance de l'environnement informatique (4.6.1.a) (4.6.1.c),
- *(4.6.1.e)* la connaissance des autres applications de notre environnement informatique (4.6.1.b),
- *(4.6.1.f)* l'identification des mécanismes par l'intermédiaire desquels notre application interagit avec son environnement et ses voisines (4.6.1.b) (4.6.1.c), ainsi que
- *(4.6.1.g)* l'évaluation de l'impact de notre application sur son environnement au sens large (incluant les autres applications) et l'effet indirect sur les critères d'évaluation de la sécurité de notre application,

et ceci pour chacun des environnements informatiques concernés[6], ce qui dans le cas d'une application réseau distribuée sur l'Internet, et tenant compte des disparités technologiques (1.1.3.a) propres à notre entreprise, s'avère difficile à appréhender. Dans la suite de ce document et chaque fois que cela s'avérera nécessaire,

[6] Soit l'environnement dans lequel sera installé le serveur ainsi que l'environnement de chaque poste client.

nous nous référerons donc à un seul de ces environnements informatiques, celui du siège central de l'entreprise *(4.6.1.h)*, choisi pour les raisons suivantes:

- nous le connaissons bien;
- ses besoins de sécurité sont élevés (liaison permanente à l'Internet, présence du LAN privé d'entreprise, lieu d'exercice de l'activité stratégique de l'entreprise (1.1.1.c));
- c'est l'endroit où devrait être installé le serveur;
- c'est le lieu probable de développement et/ou point de départ du déploiement de l'application.

4.6.2. L'environnement informatique

L'environnement informatique (4.6.1.d) de notre application est le lieu d'où proviennent les ressources dont elle a besoin pour fonctionner et qui sont principalement constituées de matériels (machines, câbles, etc.), de logiciels (systèmes d'exploitation), et d'une combinaison ou interaction des deux. Par facilité, nous utiliserons la notion de *ressources essentielles (4.6.2.a)*, définie comme l'ensemble des ressources et combinaisons de ressources nécessaires au bon fonctionnement de notre application, et dont les principales sont:

- *(4.6.2.b)* l'espace disque;
- *(4.6.2.c)* la mémoire;
- *(4.6.2.d)* le temps CPU;
- *(4.6.2.e)* l'alimentation électrique;
- *(4.6.2.f)* la bande passante;
- *(4.6.2.g)* la disponibilité[G] des matériels et logiciels;

4.6.3. Les applications voisines

Si nous considérons l'environnement témoin choisi (4.6.1.h), nous identifions 3 types d'applications voisines (4.6.1.e):

- *(4.6.3.a)* les dispositifs de protection logique de l'entreprise;
- *(4.6.3.b)* les applications liées à l'activité stratégique de l'entreprise (1.1.1.c) autres que celles visées ci-dessus (4.6.3.a);
- *(4.6.3.c)* les applications liées à l'activité normale de l'entreprise (accès et services à l'Internet) autres que celles visées ci-dessus (4.6.3.a).

Deux de ces trois types d'applications, à savoir les dispositifs de protection logique (4.6.3.a) et l'activité Internet normale (4.6.3.c), constituent par ailleurs des composantes habituelles de chaque type d'environnement.

La définition précise des qualités fondamentales, du niveau de sécurité et des vulnérabilités[G] des *dispositifs de protection logique* de l'entreprise (4.6.3.a) sort du cadre de ce document, non seulement parce que cela nous entraînerait trop loin dans un domaine différent et spécifique, mais aussi parce qu'en faire état constitue déjà en soi une atteinte à ce que nous souhaitons préserver. Pour nos besoins, nous nous contenterons donc d'en énoncer les objectifs:

- *(4.6.3.d)* assurer la protection (disponibilité[G], intégrité[G], confidentialité[G], imputabilité[G]) des logiciels et des données de l'entreprise ou des clients de l'entreprise par rapport à toute forme de menace[G] logique venant de l'Internet;
- *(4.6.3.e)* autoriser un accès contrôlé de l'intérieur de l'entreprise à l'Internet.

Sans surprise, au niveau des moyens mis en oeuvre, nous trouverons des fonctions de *proxying* et de *packet filtering* réparties sur plusieurs machines et configurées sur base du principe strict que tout ce qui n'est pas expressément autorisé est interdit *(4.6.3.f)*.

L'*activité stratégique* de l'entreprise (4.6.3.b) est représentée par une offre commerciale à trois volets:

- *(4.6.3.g)* l'hébergement d'applications informatiques (applications administratives, comptables, ERP, production, etc.) avec accès sécurisé du client via l'Internet;
- *(4.6.3.h)* l'hébergement d'applications bureautiques (traitement de texte, tableur, courrier électronique, navigateur internet, etc.) avec accès sécurisé du client via l'Internet;

- *(4.6.3.i)* le développement et l'hébergement de sites web de commerce électronique, ce qui inclut les services DNS et HTTP(S) offerts dans ce contexte à l'Internet par l'entreprise;

Enfin, l'*activité normale de l'entreprise* (4.6.3.c) consiste majoritairement aux quatre fonctions principales suivantes:

- *(4.6.3.j)* l'accès aux serveurs SMTP, DNS, FTP, NNTP et HTTP(S) de l'Internet pour les personnes travaillant derrière les dispositifs de protection logique (4.6.3.a);
- *(4.6.3.k)* l'hébergement occasionnel d'autres types de sites web (statiques ou dynamiques) que ceux visés ci-dessus (4.6.3.i), ce qui inclut les services DNS et HTTP(S) offerts dans ce contexte à l'Internet par l'entreprise;
- *(4.6.3.l)* la mise à disposition sur l'Internet de services DNS et SMTP autres que ceux visés plus haut (4.6.3.i) (4.6.3.k);
- *(4.6.3.m)* le développement et la maintenance de l'offre commerciale complète de l'entreprise (ce qui inclut les applications administratives (4.6.3.g)), ainsi que le support client.

4.6.4. Les mécanismes d'interaction

Lors de l'introduction de notre nouvelle application dans un environnement informatique préexistant, deux mécanismes d'interaction (4.6.1.f) semblent devoir jouer:

- *(4.6.4.a)* les adaptations de configuration et
- *(4.6.4.b)* la concurrence pour l'utilisation des ressources essentielles (4.6.2.a).

Les *adaptations de configuration*, si nécessaires, sont à réaliser une fois par environnement et ont pour objectif de permettre d'ajouter notre application tant à la liste des services Internet auxquels les employés de l'entreprise ont accès (4.6.3.j) qu'à la liste des services de l'entreprise auxquels nos clients seuls devraient avoir accès (2.1.3.a) (4.6.3.g) (4.6.3.h). L'*utilisation des ressources essentielles* est par contre un processus récurrent dans lequel notre application risque d'entrer en compétition avec les autres applications.

4.6.5. Evaluation de l'impact

Dans ce paragraphe, nous allons évaluer l'impact possible via les *mécanismes d'interaction* (4.6.4) sur chacune des *applications voisines* (4.6.3).

L'*adaptation de la configuration* (4.6.4.a) des *dispositifs de protection logique* (4.6.3.a) représente toujours une part de risque, que cette part soit la conséquence d'une erreur humaine, de l'ouverture de ports supplémentaires (connexions entrantes) ou de l'insertion de modules supplémentaires (proxys) ayant leurs propres vulnérabilités[G] *(4.6.5.a)*. Si, en plus, nous prenons en considération la disparité technologique (1.1.3.a) et la dispersion géographique (1.1.2.a) (1.1.2.b) de l'entreprise, nous nous trouvons dans une situation délicate où le risque[G] d'une atteinte aux objectifs desdits dispositifs de protection (4.6.3.d) (4.6.3.e) ne serait plus fonction d'un niveau de probabilité p mais de $\sum p_i$, où i représenterait le nombre d'environnements distincts interconnectés[7]. Et même si la valeur de l'expression $\sum p_i$ reste faible, l'ouverture éventuelle d'une brèche dans ces dispositifs de protection représente un risque[G] considérable *(4.6.5.b)*.

Au niveau des *activités stratégiques* de l'entreprise (4.6.3.b), la seule *adaptation de configuration* (4.6.4.a) qui pourrait être envisagée consisterait à permettre au trafic de la nouvelle application d'emprunter, quand elles existent, les connexions sécurisées[8] reliant certains de ces environnements (4.6.3.g) (4.6.3.h), connexions dont les points d'entrée se situent de part et d'autre derrière les dispositifs de protection logique (4.6.3.a). Cette possibilité toutefois ne devrait pas être retenue, puisque la bande passante allouée à ces connexions sécurisées est normalement garantie contractuellement et allouée entièrement aux applications des clients (risque[G] d'atteinte à leur disponibilité[G]) *(4.6.5.c)*.

L'installation de la nouvelle application ne semble pas devoir provoquer d'*adaptation de configuration* (4.6.4.a) au niveau des *activités normales* de l'entreprise (4.6.3.c) *(4.6.5.d)*.

[7] Chaque environnement distinct (client de l'entreprise, filiale, télétravailleur) hébergeant un poste client ou le serveur de notre application risque donc, si nous n'y prenons garde, de devoir adapter sa protection logique.
[8] Connexion du style VPN, utilisées par les clients ASP ainsi que par certains télétravailleurs.

Un problème de *concurrence pour l'utilisation des ressources essentielles* (4.6.4.b) entre notre nouvelle application et les *dispositifs de protection logique* (4.6.3.a) devrait produire des effets principalement au niveau de la disponibilité[G] de ces derniers (performances, voire interruption); ces dispositifs étant naturellement configurés selon le principe du *fail safe*, le seul impact direct à considérer serait l'allongement du délai de reporting en cas d'incident *(4.6.5.e)*. Toutefois, une dégradation significative de la disponibilité[G] des dispositifs de protection logique aurait une conséquence indirecte sur la disponibilité[G] des applications pour lesquels ces dispositifs constituent une ressource essentielle (4.6.2.g), contrevenant ainsi aux objectifs desdits dispositifs par rapport aux applications stratégiques (4.6.3.d) et normales (4.6.3.e) de l'entreprise *(4.6.5.f)*.

Un problème de *concurrence pour l'utilisation des ressources essentielles* (4.6.4.b) entre notre nouvelle application et les *applications stratégiques* de l'entreprise (4.6.3.d) aurait un impact direct sur la disponibilité[G] de ces dernières, donc par essence nous poserait un problème grave *(4.6.5.g)*. Par rapport aux *applications normales* de l'entreprise, le même raisonnement prévaut même si l'impact serait ici d'un niveau inférieur *(4.6.5.h)*.

Tableau 4.4. Evaluation de l'impact d'un problème d'écologie

Mécanisme d'interaction (4.6.4.)	*Cible du mécanisme d'interaction (4.6.3)*	*Evaluation de l'impact (cas pire)*	*Motivation principale*
Adaptation de configuration (4.6.4.a)	Dispositifs de protection logique (4.6.3.a)	3	(4.6.5.b)
	Activités stratégiques (4.6.3.b)	0	(4.6.5.c)
	Activités normales (4.6.3.c)	0	(4.6.5.d)
Partage des ressources (4.6.4.b)	Dispositifs de protection logique (4.6.3.a)	0	(4.6.5.e)
	Activités stratégiques (4.6.3.b)	2	(4.6.5.f) (4.6.5.g)
	Activités normales (4.6.3.c)	1	(4.6.5.f) (4.6.5.h)

Pour représenter les évaluations d'impacts du tableau ci-dessus sous la forme de notre tableau traditionnel, nous avons procédé comme suit:

- l'ouverture d'une brèche dans les dispositifs de protection logique de l'entreprise (4.6.5.b) est considérée comme une menace[G] affectant prioritairement l'activité stratégique de l'entreprise;
- toute valeur d'impact affectant l'activité stratégique de l'entreprise (4.6.5.f) (4.6.5.g) sera conservée telle quelle;
- tout type d'impact sur l'activité normale de l'entreprise (4.6.5.f) (4.6.5.h) se fera également ressentir sur notre nouvelle application (4.6.3.m) *(4.6.5.i)*; puisque l'impact ici est la conséquence d'une atteinte à la disponibilité[G], nous reprenons donc les valeurs d'impact estimées dans le cadre d'une atteinte à la disponibilité[G] de notre application (4.3.2).

Tableau 4.5. Evaluation de l'impact d'un problème d'écologie

Cible potentielle	*Impact*	*Motivation principale*
Objectif de réduction des coûts (2.1.1.a)	0	(4.3.2.a)
Objectif de recherche de synergies (2.1.2.a)	0	(4.3.2.a)
Objectif d'amélioration du support (2.1.3.b)	1	(4.6.5.f) (4.6.5.h) (4.3.2.b)
Image de l'entreprise (4.2.b)	1	(4.6.5.f) (4.6.5.h) (4.3.2.c)
Objectifs stratégiques de l'entreprise (1.1.1.c)	3	(4.6.5.b) (4.6.5.f) (4.6.5.g) (4.3.2.d)

4.6.6. Mesures proposées

Dans le meilleur des mondes, nous exigerions le respect des contraintes suivantes:

- *(4.6.6.a)* la nouvelle application devrait pouvoir être mise en service sans imposer de modification de configuration (4.6.4.a) des dispositifs de protection logique de l'entreprise (4.6.3.a) (4.6.5.b);
- *(4.6.6.b)* une fraction de la ressource bande passante (4.6.2.f) totale sera utilisable par la nouvelle application, qui devra veiller elle-même (4.6.6.a) à ne pas en dépasser la limite;
- *(4.6.6.c)* en cas de dégradation de la ressource bande passante (4.6.2.f) totale, la nouvelle application devra pouvoir s'adapter et céder la priorité aux autres applications;
- *(4.6.6.d)* les différentes composantes applicatives de l'environnement (4.6.3.a) (4.6.3.b) (4.6.3.c) devraient, chaque fois que possible, pouvoir utiliser des ressources propres (non partagées): la plupart des conflits potentiels de ressources pourront être évités en utilisant des matériels distincts (4.6.2.g) (4.6.2.b) (4.6.2.c) (4.6.2.d) (4.6.2.e).

Ce dernier point mérite un commentaire. Dans l'organisation actuelle de l'entreprise, les matériels et logiciels participant de la fonction de sécurité logique (4.6.3.a) n'offrent pratiquement aucun service applicatif (4.6.3.b) (4.6.3.c), et inversement, les machines dédiées aux applications n'occupent aucun rôle dans le domaine de la sécurité logique de l'entreprise (ce que ne contredisent pas les règles élémentaires de *host security*). De plus, les services HTTP(S) offerts dans le cadre de l'activité stratégique (4.6.3.i) de l'entreprise le sont par des serveurs distincts de ceux offerts dans le cadre de l'activité normale (4.6.3.k). C'est donc la continuation de ce principe de séparation des fonctions, dans les limites des ressources matérielles disponibles (1.2.3.b), qui est visée ici. Une application concrète de ce principe général qui mérite d'être signalée ici serait par exemple le point de raccordement électrique:

- (4.6.6.e) la nouvelle application n'étant pas stratégique, tout serveur qui lui serait dédié (4.6.6.d) ne pourra pas être raccordé à la partie du réseau électrique supportée par les UPS (possibilité d'impact en disponibilité[G] sur les autres applications (4.6.5.f) (4.6.5.g))

4.7. Intégrité de l'application

4.7.1. Pertinence du critère

L'intégrité[G], tout comme la confidentialité[G], peut s'envisager à différents niveaux:

- *(4.7.1.a)* l'intégrité[G] du code (source ou binaire) de l'application;
- l'intégrité[G] des données de l'application:
  - intégrité[G] des données persistantes:
    - *(4.7.1.b)* paramètres de connexion[G] (identifiant et mot de passe, par exemple) (4.4.1.d) et
    - *(4.7.1.c)* profils utilisateurs (attributs divers de l'utilisateur) (4.4.1.e);
  - intégrité[G] des données non persistantes:
    - *(4.7.1.d)* le contenu des conversations (4.4.1.f) et
    - *(4.7.1.e)* l'identité des participants à une conversation (4.4.1.g);
- *(4.7.1.f)* l'intégrité[G] des protocoles (échanges) de l'application.

4.7.2. Evaluation de l'impact

Une atteinte à l'intégrité[G] du code source de l'application (4.7.1.a) pourrait, si ce code était recompilé, avoir des conséquences à tous les niveaux sur la disponibilité[G] (4.3.2.b) (4.3.2.c) *(4.7.2.a)*, la confidentialité[G] (4.4.2.d) (4.4.2.e) (4.4.2.f) (4.4.2.g) *(4.7.2.b)*, l'imputabilité[G] (4.5.2.a) (4.5.2.b) (4.5.2.c) (4.5.2.d) *(4.7.2.c)*, l'écologie[G] (4.6.5.f) *(4.7.2.d)* de l'application ainsi que sur l'intégrité[G] de ses différents types de données et de protocoles (4.7.1.b) (4.7.1.c) (4.7.1.d) (4.7.1.e) (4.7.1.f). Pour ce qui est du code binaire, une atteinte directe à son intégrité[G] ne devrait en général porter atteinte qu'à la disponibilité[G] (4.3.2.b) (4.3.2.c) totale ou partielle de l'application *(4.7.2.e)*.

Une atteinte à l'intégrité[G] des paramètres de connexion[G] (4.7.1.b) pourrait avoir des répercussions en disponibilité[G] (4.3.1.b) *(4.7.2.f)* et en imputabilité[G] (4.5.1.g) *(4.7.2.g)*; une atteinte à l'intégrité[G] des profils des

utilisateurs pourrait permettre à un client d'obtenir une visibilité des autres utilisateurs qui lui serait autrement impossible, d'où problème de confidentialité[G] (4.4.2.d) *(4.7.2.h)*; elle pourrait également permettre à certaines catégories d'utilisateurs d'accéder à des privilèges supplémentaires (conversations entre clients, par exemple, ce qui ne doit normalement pas être possible (3.1.d), d'où atteinte en disponibilité[G] [9]) *(4.7.2.i)*. Une atteinte à l'intégrité[G] du contenu des conversations (4.7.1.d) n'aura, si elle reste réduite, a priori aucun effet mais en s'intensifiant pourrait provoquer un problème de disponibilité[G] (4.3.1.d) *(4.7.2.j)*. Une atteinte à l'intégrité[G] des données identifiant les participants à une conversation (4.7.1.e) aurait probablement, sous réserve d'une analyse ultérieure des protocoles utilisés, au moins un effet possible sur la disponibilité[G] (4.3.1.a) (4.3.1.b) (4.3.1.d) *(4.7.2.k)* et l'imputabilité[G] *(4.7.2.l)*.

Enfin, une atteinte à l'intégrité[G] des protocoles de l'application (4.7.1.f) pourra avoir un impact différent selon le type de protocole atteint, c'est à dire comme en (4.4.2) selon le type de données véhiculées[10]:

- *(4.7.2.m)* dans le cas des protocoles véhiculant principalement les données persistantes (profils (4.7.1.c) et paramètres de connexion[G] (4.7.1.b) des utilisateurs), les conséquences d'une atteinte à leur intégrité[G] seraient de l'ordre de la disponibilité[G], de l'imputabilité[G] et de la confidentialité[G] (4.7.2.b) (4.7.2.c);
- *(4.7.2.n)* dans le cas des protocoles véhiculant principalement les données non persistantes (contenu des conversations, identité des participants à une conversation), les conséquences d'une atteinte à leur intégrité[G] seraient de l'ordre de la disponibilité[G] et de l'imputabilité[G] (4.7.2.d) (4.7.2.e).

On le voit, l'impact d'un problème d'intégrité[G] est principalement indirect, ses conséquences directes consistant habituellement en l'altération d'une autre des propriétés de sécurité attendues de notre application. L'évaluation de cet impact ressemble à ce que donnerait une fonction 'maximum' appliquée sur les tableaux des impacts de disponibilité[G], confidentialité[G], imputabilité[G] et écologie[G] (limitée, dans ce dernier cas, aux effets de la concurrence sur les ressources (4.6.5.f)).

Tableau 4.6.	**Evaluation de l'impact d'un problème d'intégrité**	
Cible potentielle	*Impact*	*Motivation principale*
Objectif de réduction des coûts (2.1.1.a)	1	C
Objectif de recherche de synergies (2.1.2.a)	1	C+W
Objectif d'amélioration du support (2.1.3.b)	2	D+C+W+E
Image de l'entreprise (4.2.b)	1	D+C+W+E
Objectifs stratégiques de l'entreprise (1.1.1.c)	2	C+W

4.7.3. Mesures proposées

Les mesures à prendre consistent à rendre, chaque fois que c'est possible, le code (source) et les données de l'application inaccessibles ou inutilisables:

- *(4.7.3.a)* chaque fois que c'est possible, ne pas distribuer de code source sur les machines des utilisateurs (découpe de l'application en modules);
- *(4.7.3.b)* si du code source devait être disponible (distribué ou désassemblé), s'assurer que sa divulgation ne fournisse pas d'indications facilitant une atteinte à l'intégrité[G] de l'application;
- *(4.7.3.c)* si du code source devait être disponible (distribué ou désassemblé), s'assurer que l'impact d'une modification éventuelle de celui-ci ne se produise qu'en termes de disponibilité[G] de l'application depuis le module et/ou pour l'utilisateur concerné(s);
- *(4.7.3.d)* ne pas conserver de données persistantes (4.7.1.b) (4.7.1.c) sur les machines des utilisateurs;
- *(4.7.3.e)* les phases éventuelles de conception, développement et qualification de l'application devront être effectuées dans un environnement rigoureusement protégé;

4.8. Conclusions

Contre toute attente pour une application de type multimédia, c'est la propriété d'intégrité[G] qui se trouve la plus fréquemment citée parmi celles dont l'altération produirait l'impact le plus important (tableau 4.7, colonne de droite). Seconde surprise, ce sont des considérations d'écologie[G], par le biais d'erreurs

[9] Considérant que le nombre de communications simultanées est limité (4.3.3.g) (4.3.3.h).

[10] Faisant ici abstraction des mesures éventuellement déjà proposées par ailleurs (notamment en 4.4.3).

consécutives à des modifications de configuration des dispositifs de protection logique, qui représentent la menace[G] la plus grave pour l'entreprise (avant-dernière colonne) *(4.8.a)*.

Si nous regardons maintenant les différentes lignes de ce tableau, nous voyons que sur l'ensemble des critères notre plus grande vulnérabilité[G] se situe par rapport aux objectifs stratégiques de l'entreprise juste avant l'objectif d'amélioration du support. Et ici également, le poids du critère d'écologie[G] semble déterminant (4.8.a).

Tableau 4.7. Synthèse des impacts évalués							
Cibles de protection 3.2	*D 3.3*	*C 3.4*	*W 3.5*	*E 3.6*	*I 3.7*	*Max*	*Critères dominants*
Objectif de réduction des coûts (2.1.1.a)	0	1	0	0	1	**1**	C+I
Objectif de recherche de synergies (2.1.2.a)	0	1	1	0	1	**1**	C+W+I
Objectif d'amélioration du support (2.1.3.b)	1	1	2	1	2	**2**	W+I
Image de l'entreprise (4.2.b)	1	1	1	1	1	**1**	D+C+W+E+I
Objectifs stratégiques de l'entreprise (1.1.1.c)	0	2	1	3	2	**3**	E
Max	**1**	**2**	**2**	**3**	**2**	**3**	
Impacts principaux	(2.1.3.b) (4.2.b)	(1.1.1.c)	(2.1.3.b)	(1.1.1.c)	(2.1.3.b) (1.1.1.c)		

Il conviendrait toutefois de pondérer ces conclusions par la quantification, ou probabilité réelle de survenance d'un type de sinistre. Après tout, les adaptations de configuration des dispositifs de protection logique ne sont à effectuer qu'une fois; si celles-ci sont opérées de manière et avec un contrôle rigoureux le risque[G] d'erreur peut devenir extrêmement faible[11]. De même, l'occurrence directe d'un problème de confidentialité[G] semble devoir être plus élevée que celle d'une atteinte à l'intégrité[G] du code source de l'application avant compilation et déploiement (4.7.2.a), même si ce dernier cas de figure demeure préoccupant *(4.8.b)*.

En remontant à l'analyse des critères et tenant compte de l'occurrence possible des différents types de sinistre, cette évaluation de nos besoins en matière de sécurité nous paraît mettre en évidence, dans l'ordre décroissant de pertinence, cinq aspects fondamentaux:

- *(4.8.c) écologie*[G]: une attention toute particulière sera à porter à la problématique du partage de la bande passante (4.6.5.f) (4.6.5.g);
- *(4.8.d) confidentialité*[G]: au niveau des conversations bien sûr (4.4.3.h), mais aussi de la visibilité externe (4.4.3.b) et interne (4.4.3.c) des participants aux dites conversations;
- *(4.8.e) imputabilité*[G]: importance de l'authentification[G] de l'utilisateur
- *(4.8.f) intégrité*[G]: les risques[G] principaux semblent se situer autour des problèmes d'intégrité[G] du code (4.7.3.a) (4.7.3.b) et des données persistantes (4.7.3.d);
- *(4.8.g) écologie*[G]: enfin, si elles ne peuvent être évitées, les adaptations aux dispositifs variés de protection logique de l'entreprise devront être effectuées avec le plus grand soin (4.6.5.b).

Ce qui donne, pour les critères mis en évidence sur le tableau qui précède, une hiérarchisation à peu près inverse de celle suggérée par ledit tableau.

Notons encore le rôle relativement marginal du critère de disponibilité[G] *(4.8.h)*.

[11] Ce qui n'atténue toutefois pas le risque d'introduction de nouvelles vulnérabilités[G] (4.6.5.a).

Chapitre 5 La méthode EBIOS

Dans ce chapitre, nous allons envisager l'utilisation d'une méthode de détermination des besoins de sécurité que nous avons envisagée plusieurs semaines après avoir rédigé le chapitre précédent: la méthode EBIOS. L'occasion de consolider notre démarche.

5.1. Introduction

5.1.1. Avertissement

Dès lors qu'il s'agit d'exploiter une méthode un tant soit peu élaborée, nous nous trouvons confrontés à un certain nombre de limitations inhérentes au profil particulier de notre projet (1.2.3) et du contexte académique dans lequel il s'inscrit, limitations dont les trois principales nous paraissent être:

- la confusion de rôles: utilisateur, développeur, responsable de la sécurité, administrateur, décideur, auditeur, sont autant de rôles distincts assumés, dans notre cas, par une seule personne. Pour palier cet inconvénient, nous tenterons - chaque fois que cela s'avérera possible - de nous positionner dans le rôle de l'intervenant principal de l'étape en cours pour la méthode envisagée;
- la limitation des informations: si les informations de nature technique nous sont généralement accessibles, il n'en va pas de même du détail des plans stratégiques, ni de l'organisation et de la structure financières de l'entreprise; nous serons donc contraints, le cas échéant, de faire l'impasse sur certains éléments;
- les limites, en termes de ressources mobilisables et de volume du document final, liées au contexte académique susmentionné.

Le lecteur ne s'étonnera donc pas que les méthodes visitées le soient à grandes enjambées, dans un effort consistant à aller directement à ce qui nous paraît l'essentiel.

5.1.2. Pourquoi EBIOS

Nous avons choisi de nous intéresser à la méthode EBIOS pour les raisons suivantes:

- il ne s'agit pas d'une des nombreuses méthodes commerciales utilisées ou commercialisées par l'une ou l'autre société privée, mais du résultat d'une initiative publique avec la disponibilité[G] et le retentissement potentiel que cela peut signifier;
- une documentation existe et est disponible gratuitement;
- un logiciel de mise en oeuvre existe et est disponible gratuitement[12];
- les résultats de la mise en oeuvre de la démarche EBIOS peuvent être transposés vers d'autres méthodes[13].

5.1.3. Contexte historique

La réflexion autour de la sécurité et de l'évaluation de la sécurité des SI ne date pas d'hier, et on peut raisonnablement considérer que c'est au début des années 1980, avec la publication aux Etats-Unis des TCSEC ("orange book") [TCSEC], qu'elle a produit ses premiers résultats significatifs à échelle internationale. En Europe, c'est à l'instigation de la Commission Européenne au début des années 1990 qu'un premier effort de normalisation des critères français, allemands et anglais (UK Confidence Levels [CESG89]) menait à la publication de la norme ITSEC 1.2 (1991) [ITSEC] .

Parallèlement à sa participation au projet ITSEC, le SCSSI a mis en place dès 1990 une démarche et un ensemble de guides visant à aider les concepteurs de SI à réaliser des systèmes susceptibles de remplir les

[12] Le code source, en java, est également distribué.
[13] Certaines de ces méthodes sont citées dans l'ANNEXE 1.

conditions nécessaires à une évaluation ITSEC. La méthode EBIOS (*Expression des Besoins et Identification des Objectifs de Sécurité*) est une des résultantes de cette démarche.

5.1.4. Positionnement de la méthode dans le cycle de vie

Par rapport au modèle simplifié de cycle de vie proposé par l'ITSEC (modèle composé des phases de *spécification des besoins*, de *conception*, de *réalisation* et d'*utilisation*), la méthode EBIOS se rapporte à la seule *spécification des besoins*. Une représentation du positionnement de l'ensemble des guides et méthodes issus de la démarche du SCSSI par rapport audit modèle simplifié figure en ANNEXE 1.

5.1.5. Audience

La méthode EBIOS s'adresse d'une part aux utilisateurs et responsables de (parties de) systèmes qu'elle assiste dans leur démarche d'expression des besoins de sécurité, ainsi qu'au(x) responsable(s) de la sécurité chargé(s) d'effectuer la synthèse finale des objectifs de sécurité. La personne responsable de conduire l'étude est l'*évaluateur (5.1.5.a)*.

5.1.6. Matériel

Pour notre étude, nous avons utilisé la documentation relative à la version 1.02 de la méthode EBIOS (Février 1997) disponible sur le *serveur thématique de la sécurité des systèmes d'information* (http://www.ssi.gouv.fr), service du Premier Ministre de la République française. Cette documentation est constituée des éléments suivants:

- un guide, contenant l'introduction et le glossaire [EB-G]
- le descriptif de la démarche par étape et activité (*que faire ?*) [EB-D]
- un catalogue de techniques (*comment le faire ?*) [EB-T]
- une base de données de connaissance (*avec quoi le faire ?*) [EB-O]
- le logiciel d'accompagnement de la méthode (la version que nous avons utilisée était la 1.5), disponible sur simple demande, accompagné d'une étude de cas.

5.1.7. Principe

La démarche EBIOS consiste en une approche relativement structurée mais non formelle constituée de 4 étapes dont deux seulement nous intéressent ici: *l'étude du contexte* et *l'expression des besoins de sécurité*. Chacune de ces étapes se décline ensuite en un certain nombre d'activités décrites dans la partie *démarche* du guide [EB-D] selon une structure normalisée reprenant chaque fois:

- un organigramme reprenant la dynamique de l'activité;
- la description de l'activité;
- la liste des données en entrée;
- la liste des données en sortie;
- les préalables à l'activité;
- les actions de l'activité;
- les savoir-faire mis en oeuvre (référence à la partie *techniques* de la documentation [EB-T]);
- les outils utilisables (référence à la partie *outillage* de la documentation [EB-O]).

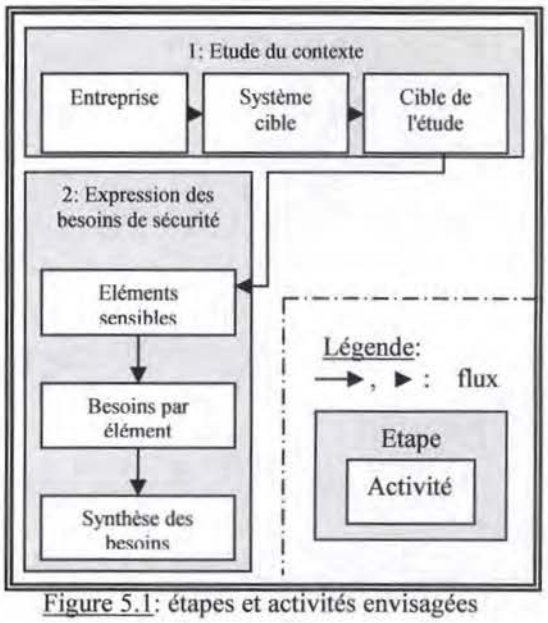


Figure 5.1: étapes et activités envisagées

La première étape, l'*étude du contexte*, est comme son nom l'indique destinée à cerner l'environnement du SC (*système cible*, but de l'étude), et à positionner ce dernier dans l'ensemble du SI de l'entreprise. L'*expression des besoins de sécurité* (deuxième étape) consiste à la définition progressive du SC en termes d'éléments sensibles (fonctions et informations) et à l'estimation des besoins de sécurité pour chacun de ces éléments.

5.2. Etape 1: l'étude du contexte

5.2.1. Présentation de l'étape

L'étude du contexte est destinée à permettre d'identifier le SC de manière globale et de le positionner par rapport à son environnement. Cette étape est composée des 3 activités suivantes:

- l'étude de l'entreprise[14],
- l'étude générale du SC et
- la détermination de la cible de l'étude de sécurité.

L'*étude de l'entreprise* consiste principalement à dessiner le profil de l'entreprise selon trois angles de vue:

- celui d'une présentation officielle classique (nom, chiffre d'affaire, etc.) mais intégrant aussi la description du métier, des missions et des valeurs de l'entreprise;
- via un aperçu de son organisation générale (structure, organigramme);
- par l'expression de la liste des contraintes diverses (culturelles, stratégiques, techniques, etc.) qui le caractérisent.

EBIOS offre, pour chacune de ces visions, une liste de rubriques et/ou un questionnaire appropriés.

L'*étude générale du SC* correspond à une définition progressive du SC à partir de la définition du SI de l'entreprise. Cette approche procède par paliers qui consistent successivement à:

- dessiner l'architecture conceptuelle du SI global de l'entreprise, c'est-à-dire identifier les différents domaines (par exemple la gestion administrative, la gestion des relations commerciales, etc.) ainsi que les acteurs extérieurs à ces domaines (clients, entreprises, organismes divers, etc.);
- sélectionner, dans ce dessin d'architecture, les éléments qui font partie du SC (éventuellement déjà existants ou non) et identifier les relations du SC avec le reste du SI de l'entreprise;
- définir le SC en termes
  - d'éléments essentiels: fonctions et catégories d'informations du SC;
  - d'enjeux de politique générale du SI, d'enjeux de politique générale de sécurité, et de contraintes ou d'exigences particulières pesant sur le SC.

Enfin, *la détermination de la cible de l'étude de sécurité* vise à définir les entités sur lesquelles s'appuie la réalisation des mesures de sécurité. Elle consiste en l'identification exhaustive des moyens (matériels, logiciels, personnels, organisationnels et procéduraux, réseaux, sites d'implantation, etc.) mis à contribution par le SC, puis en l'établissement de deux tableaux de références croisées établissant l'existence (ou non) d'une relation entre:

- chaque moyen identifié et chaque fonction essentielle du SC (premier tableau);
- chaque moyen identifié et chaque catégorie d'informations essentiels du SC (second tableau).

Ces deux tableaux constituent l'aboutissement de la première étape EBIOS et définissent la cible de l'étude.

5.2.2. Etape 1 - Activité 1: étude de l'entreprise

La première colonne du tableau 5.1 page suivante reprend en caractères gras les éléments d'appréciation issus des techniques EBIOS [EB-T]; lorsque l'élément de cette colonne est écrit en caractères italiques, il s'agit d'un élément que nous avons ajouté.

[14] EBIOS utilise l'appellation plus générique d'*organisme*, appellation que par souci d'homogénéité nous avons remplacée par celle d'*entreprise*.

Tableau 5.1	**Synthèse des éléments stratégiques**
1. - Présentation de l'entreprise	
Métier	Editeur de logiciels et prestataire de services informatiques (1.1.1.b).
Missions	1. - Développer et vendre des applications administratives (comptabilité, ERP) (1.1.1.b). 2. - Héberger ces applications en mode ASP (accès sécurisé via l'Internet) (1.1.1.c). 3. - Développer et héberger des sites Internet d'e-commerce B2B (1.1.1.c).
Présentation	PME dont le siège central emploie une dizaine de personnes (1.1.1.a) et qui est installée dans plusieurs pays (1.1.2.a).
Stratégie	Axée sur l'Internet (les missions 2 et 3) (1.1.1.c).
Valeurs	1. - *(5.2.2.a) Engagement*: la relation client - fournisseur est atypique, plus proche du partenariat et souvent doublée de relations personnelles. *2. - (5.2.2.b) Autonomie*: les employés disposent d'une grande autonomie d'organisation de leur travail.
Vocation	Société commerciale, secteur tertiaire, prestataire de services pour l'industrie, la finance et la distribution.
2. - Organisation générale	
Coordination	*(5.2.2.c)* Ajustement mutuel.
Organigramme	Aucun organigramme officiel n'existe; au niveau opérationnel (production et soutien), les prérogatives sont habituellement liées aux compétences (produits).
Structure	*(5.2.2.d)* Organique (souple) derrière le Directeur Général qui assure les niveaux décisionnels (stratégie) et de pilotage (gestion, parfois coordination).
3. - Contraintes générales	
Budgétaires	Il n'y a pas de budget disponible (1.2.3.b) pour une activité non stratégique (1.2.3.a).
Calendaires	n/a
Conjoncturelles	n/a
Culturelles	*(5.2.2.e)* la problématique de la sécurité est récente dans la culture de l'entreprise.
Fonctionnelles	n/a
Implantation	*(5.2.2.f)* Certains bâtiments et locaux ne sont pas toujours très adaptés à l'utilisation qui en est faite.
Légales	n/a
Méthodes	n/a
Personnel	1. - personnel insuffisant par rapport aux missions à pourvoir (1.2.3.b). 2. - personnel insuffisamment formé par rapport aux exigences technologiques des missions stratégiques.
Politiques	n/a
Stratégiques	Les missions ciblent en priorité des comptes internationaux (volonté de dépasser les frontières nationales) (1.1.2.a).
Structurelles	La faible centralisation opérationnelle a induit une importante disparité technologique (1.1.3.a) au sein de l'organisation.
Techniques	n/a
Territoriales	Dispersion des sites d'exercice de l'activité: filiales (1.1.2.a), télétravailleurs (1.1.2.b) et personnel nomade (1.1.2.c).

Le SC est destiné à servir de support aux missions (développement) et aux valeurs (5.2.2.a) de l'entreprise.

5.2.3. Etape 1 - Activité 2: étude du système cible (SC)

5.2.3.1. Architecture conceptuelle du SI

Le SI de l'entreprise se compose de plusieurs domaines d'activité avec lesquels interagissent un certain nombre d'acteurs externes, illustrés par la figure 5.2 qui est représentative de certaines valeurs (5.2.2.a), de la structure (5.2.2.d) et du mode de coordination (5.2.2.c) de l'entreprise: à quelques rares exceptions près, tout le monde interagit avec tout le monde.

La figure 5.2 ne représente pas les relations entre acteurs externes, hors de notre propos. A noter que si les commerciaux (vendeurs) ne font pas à proprement parler partie du personnel de l'entreprise, ils sont pourtant bien perçus comme tels par les clients et réalisent parfois eux-mêmes certaines tâches techniques et de

support; pour cette raison, dans la suite de notre étude nous les assimilerons au personnel de l'entreprise *(5.2.3.1.a)*.

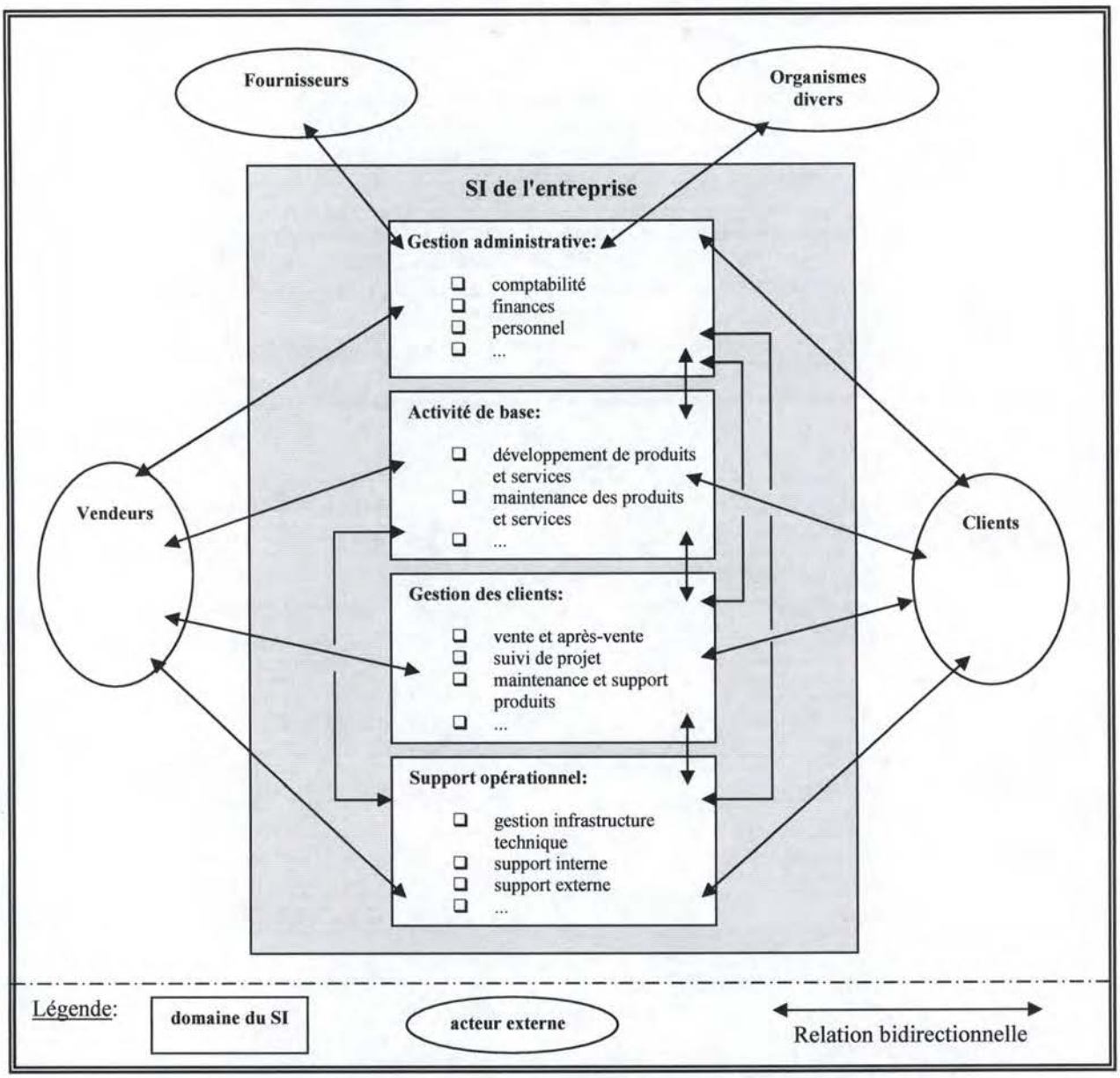


Figure 5.2: domaines du SI de l'entreprise et acteurs externes

5.2.3.2. Identification du SC

Le SC, en tant qu'outil dont la finalité n'est autre que la communication, ne représente pas un nouveau domaine du SI de l'entreprise, mais plutôt un support à la communication (support aux relations bidirectionnelles de la figure 5.2). Si nous revisitons les objectifs opérationnels du SC [(3.1.a) (3.1.b)], il apparaît clairement que ce support à la communication concernera les relations entre:

- (le personnel de) tous les domaines du SI à l'exception de la gestion administrative,
- les clients et
- les vendeurs [(5.2.3.1.a)].

EBIOS nous offre également la possibilité, à ce stade, de découper le SC en plusieurs sous-systèmes, sur base d'une liste de critères qui comprend:

- l'architecture matérielle (par exemples, machines ou groupes de machines distinctes coopérant par l'intermédiaire d'un réseau local);
- l'architecture fonctionnelle (répartition des fonctions ou catégories d'informations sensibles);
- l'autonomie de gestion et de responsabilité;
- l'implantation géographique (bâtiments distincts).

Malgré la taille modeste de notre application, force nous est de constater que des quatre critères évoqués ci-dessus trois sont de nature à justifier la découpe de notre système en sous-systèmes (le premier et les deux derniers). Sur base de la représentation symbolique du SC établie à la figure 5.3, que nous considérons comme une hypothèse de travail vraisemblable, nous identifions 3 sous-systèmes distincts:

- *(5.2.3.2.a)* le sous-système *serveur*, composé du serveur du SC et des éléments environnants (LAN de la DMZ et connexion WAN[15]) et situé au sein des locaux de l'entreprise (4.4.3.f),
- *(5.2.3.2.b)* le sous-système *local*, composé par les éléments du LAN privé de l'entreprise (nombreux utilisateurs), et
- *(5.2.3.2.c)* les sous-systèmes *distants* comportant chacun un ou plusieurs[16] utilisateurs distants (clients, télétravailleurs, etc.).

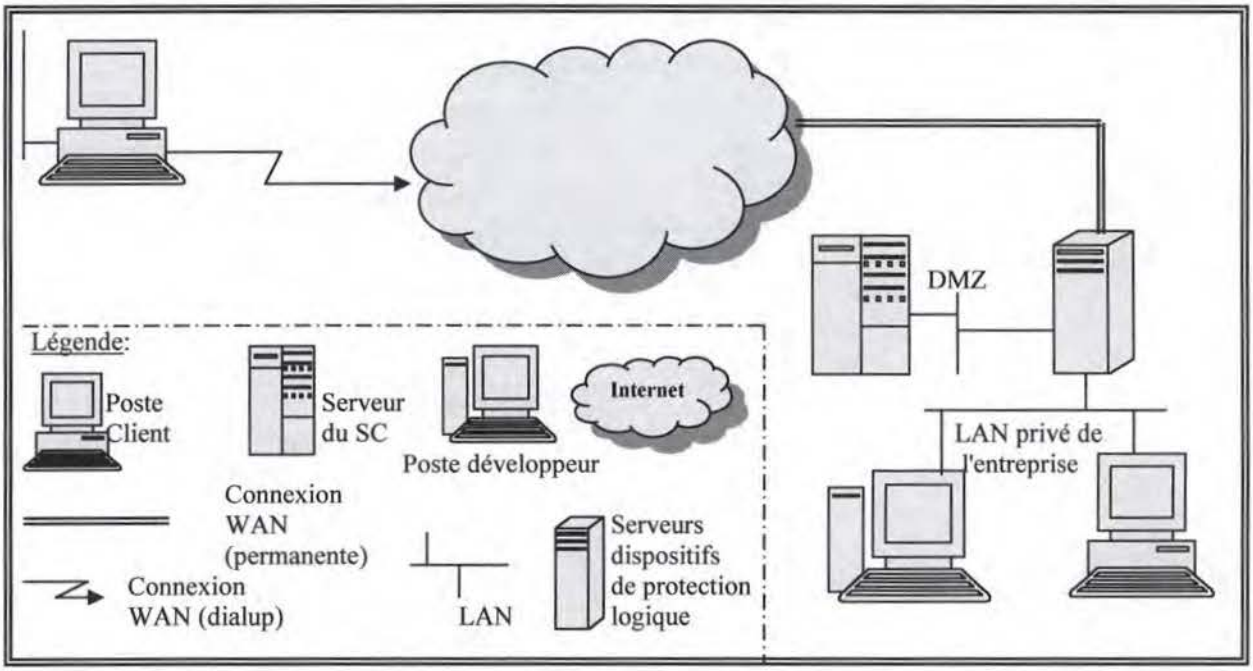


Figure 5.3: représentation symbolique de l'architecture du SC

5.2.3.3. *Représentation fonctionnelle du SC*

Le SC s'insèrera dans le SI de l'entreprise en y ajoutant un certain nombre de fonctions, lesquelles utiliseront diverses catégories d'informations. Ces fonctions et catégories d'informations dites *essentielles* sont identifiées au tableau 5.2 page suivante.

5.2.3.4. *Enjeux du SC dans le fonctionnement du SI*

Il ne nous reste plus à présent, avant de clôturer cette activité, qu'à définir les enjeux du SC par rapport à son futur environnement, c'est-à-dire:

- du point de vue de la politique générale du SI,
- du point de vue de la politique de sécurité interne et enfin
- par rapport à certaines contraintes qui lui seraient propres.

[15] Le premier critère nous permettrait même de scinder le sous-système *serveur* en deux, mais cette scission ne nous semble pas de nature à fournir à la démarche une quelconque valeur ajoutée.
[16] Dans la majorité des cas les sous-systèmes distants abriteront un ou deux utilisateurs du SC.

Les enjeux du SC en termes de *politique générale du SI* de l'entreprise ont déjà été évoqués aux chapitres précédents. Nous renvoyons donc le lecteur aux paragraphes traitant de la place du projet dans l'entreprise (1.2.3) et des objectifs généraux du projet (2.1), mais aussi à certaines considérations du chapitre 4 comme, par exemple, l'impact d'un problème de disponibilité[G] d'une application pourtant non stratégique dès lors qu'elle a été proposée aux clients comme outil d'amélioration du support (4.3.2.b) (4.3.2.c).

Tableau 5.2	**Fonctions et catégories d'informations essentielles du SC**
1. - Fonctions essentielles de l'application	
F_COMM	*(5.2.3.3.a)* La communication (3.3.5) est la fonction (et finalité) unique du SC.
F_ENROL	*(5.2.3.3.b)* L'enrôlement des utilisateurs (3.3.6.a) représente la fonction de gestion / administration du SC.
F_DEVEL	*(5.2.3.3.c)* Le développement du SC (3.3.1.a) [17].
F_DEPLO	*(5.2.3.3.d)* Le déploiement du SC (3.3.1.b) [18].
2. - Catégories d'informations essentielles	
I_AUTH	*(5.2.3.3.e)* Les données nécessaires à l'identification / authentification (3.3.2.a) des utilisateurs (typiquement, un identifiant et un mot de passe: données persistantes, *paramètres de connexion* (4.4.1.d) (4.7.1.b)).
I_PROFIL	*(5.2.3.3.f)* Les profils des utilisateurs (3.3.6.a), par exemple leur identité réelle, leur qualité de client ou d'employé, leur état (figure 3.2), etc. (données persistantes, *profils utilisateurs* (4.4.1.e) (4.7.1.c)).
I_COMM	*(5.2.3.3.g)* Le contenu des conversations pendant la communication (3.3.5) (*données non persistantes* (4.4.1.f) (4.7.1.d)).
I_CODSRC	*(5.2.3.3.h)* Le code source de l'application (4.4.1.c) (4.7.1.a).
I_CODBIN	*(5.2.3.3.i)* Le code binaire de l'application (4.7.1.a).
I_PARAM	*(5.2.3.3.j)* Informations de configuration et/ou paramétrage du SC lui-même (par exemple (4.3.3.g) (4.3.3.h)).

Pour ce qui est de la *politique de sécurité interne* force nous est de constater que nous arrivons ici aux limites de ce que notre devoir de réserve nous permet d'exprimer. Nous considèrerons donc, sans entrer dans trop de détails, que la politique de sécurité interne se caractérisée par les éléments suivants:

- *(5.2.3.4.a)* quoique récente (5.2.2.e), la prise de conscience de la problématique de la sécurité au niveau de l'entreprise et de son personnel est optimale et parfaitement intégrée;
- *(5.2.3.4.b)* la protection de la salle des serveurs contre les accidents physiques[19], les événements naturels[20] et les pertes de services essentiels (à l'exception de la connexion à l'Internet)[21] est réputée optimale;
- *(5.2.3.4.c)* l'implémentation du principe de configuration des dispositifs de protection logique (4.6.3.f) est optimale.

Même s'il nous paraît quelque peu prématuré d'entrer déjà dans des considérations aussi concrètes, la nature du SC (outil de communication via l'Internet) nous incite à penser que l'enjeu principal de politique de sécurité interne consistera à pouvoir déployer le SC tout en respectant l'intégrité de la configuration de la protection logique de l'entreprise *(5.2.3.4.d)*.

Pour terminer, les enjeux du SC *par rapport à certaines contraintes qui lui seraient propres* - entendez qui ne correspondraient pas aux contraintes générales affectant l'entreprise dont il a été question en (5.2.2) - ont été repris au tableau 5.3 page suivante.

[17] Le lecteur objectera avec raison que cette fonction fait partie d'un autre domaine du SI (Activité de base, figure 5.2). Nous avons choisi de l'inclure ici malgré tout à cause du lien conditionnant l'existence même de cette fonction au projet de SC, et de la dépendance de ce dernier par rapport à elle.

[18] Le lecteur objectera avec raison que cette fonction fait partie d'un autre domaine du SI (Activité de base, figure 5.2). Nous avons choisi de l'inclure ici malgré tout à cause du lien conditionnant l'existence même de cette fonction au projet de SC, et de la dépendance de ce dernier par rapport à elle.

[19] Accidents de type A1 (grille du CEA, ANNEXE 4).

[20] Accidents de type A3 (grille du CEA, ANNEXE 4).

[21] Accidents de type A4 (grille du CEA, ANNEXE 4), sauf coupure de la connexion à l'Internet.

Tableau 5.3	Contraintes et exigences supplémentaires
Contraintes particulières sur le SC	
Budgétaires	n/a
Calendaires	*(5.2.3.4.e)* Pas d'échéance à respecter, mais pas non plus de ressources disponibles (1.2.3.b).
Conjoncturelles	n/a
Culturelles	n/a
Fonctionnelles	n/a
Implantation	*(5.2.3.4.f)* SC distribué: prêter attention aux problèmes du déploiement, d'enrôlement, etc.
Légales	n/a
Méthodes	n/a
Personnel	*(5.2.3.4.g)* Le personnel n'est pas expérimenté pour ce genre de projet / technologie.
Politiques	n/a
Stratégiques	*(5.2.3.4.h)* Le projet ne fait pas partie de la stratégie de l'entreprise (1.2.3.a).
Structurelles	n/a
Techniques	*(5.2.3.4.i)* Vu la disparité technologique (1.1.3.a), il existe un réel besoin de portabilité.
Territoriales	n/a

5.2.4. Etape 1 - Activité 3: détermination de la cible de l'étude

5.2.4.1. Identification des entités sur lesquelles s'appuie le SC

L'identification des entités sur lesquelles s'appuie le SC nous impose au préalable de formaliser certaines hypothèses qui peuvent être considérées comme vraisemblables concernant l'architecture et le déploiement du SC, hypothèses déjà implicitement ou explicitement introduites lors de la découpe du SC en sous-systèmes (figure 5.3) et dans certains des chapitres précédents:

- *(5241a)* le SC sera constitué d'un serveur et d'un certain nombre de clients;
- *(5241b)* le serveur sera hébergé dans les locaux de l'entreprise (sous-système *serveur* (4.4.3.f) (5.2.3.2.a));
- *(5241c)* le serveur sera accessible depuis l'Internet via la ligne louée de l'entreprise (connexion WAN) (sous-système *serveur*);
- *(5241d)* le serveur sera séparé de l'Internet par un certain nombre de dispositifs de protection logique (sous-système *serveur*);
- *(5.2.4.1.e)* le SC sera développé et / ou qualifié et / ou déployé et / ou maintenu sur / depuis un poste de travail situé dans le LAN privé de l'entreprise (sous-système *local* (5.2.3.2.b));
- les types de matériel, de logiciel, de configuration et d'accès à l'Internet du côté des clients sont a priori variés; dans un souci de simplification, nous considérerons que le client type est
  - *(5.2.4.1.f)* soit un des clients intra muros (sis dans le LAN privé de l'entreprise: sous-système *local*),
  - *(5.2.4.1.g)* soit un client externe, situé dans un LAN ou pas, et utilisant toute forme de dialup Internet (sous-système *distant* (5.2.3.2.c)).

Sur base de la figure 5.3, nous avons repris au tableau 5.4 les principales entités exploitées par le SC. Pour chacune, il nous a semblé intéressant d'ajouter un indicateur visant à quantifier le niveau de confiance (hors panne matérielle ou logicielle) que nous pouvions lui accorder selon une échelle simple à trois niveaux:

- niveau 0: *hostile* - nous n'avons aucun moyen d'y contrôler quoi que ce soit;
- niveau 1: *non sécurisé* - nous disposons de certains moyens de contrôle ou d'influence;
- niveau 2: *sécurisé* - totalement sous notre contrôle.

Dans le tableau 5.4 (page suivante), les différences entre les valeurs de confiance attribuées aux entités liées respectivement aux sous-systèmes *serveur* (5.2.3.2.a) et *local* (5.2.3.2.b) peuvent paraître surprenantes: elles témoignent simplement de certaines réalités d'implantation (5.2.2.f) *(5.2.4.1.h)*.

5.2.4.2. *Représentation des liens fonctions / entités et informations / entités*

Les liens existants entre les fonctions et les entités contribuant à leur réalisation d'une part, et entre les catégories d'informations et les entités contribuant à leur traitement[22] d'autre part sont matérialisés par le tableau 5.5. Ce tableau tient compte des hypothèses formulées en (5.2.4.1) mais aussi des nouvelles hypothèses suivantes:

- *(5.2.4.2.a)* toutes les fonctions de communication (3.3.5) transitent par le serveur du SC;
- *(5.2.4.2.b)* l'enrôlement[G] est effectué localement sur le serveur du SC par l'administrateur (4.4.3.d) (4.4.3.g) du SC.
- *(5.2.4.2.c)* les données persistantes (I_AUTH (5.2.3.3.e), I_PROFIL (5.2.3.3.f) et I_PARAM (5.2.3.3.j)) ne sont pas conservées sur les postes clients (4.4.3.e);
- *(5.2.4.2.d)* le code source n'est pas déployé (4.7.3.a);
- *(5.2.4.2.e)* le déploiement du code binaire est effectué par l'administrateur via les réseaux (LAN/WAN);
- *(5.2.4.2.f)* les paramètres de connexion[G] (I_AUTH (5.2.3.3.e)) et de configuration (I_PARAM (5.2.3.3.j)) ne transitent pas sur les réseaux (4.4.3.d);

Tableau 5.4	**Entités du SC**	*(localisation sur base des hypothèses en 5.2.4.1)*
1. - Ressources matérielles		
Ressource	*Confiance*	*Description*	*S/Système*
E_S_SVHW	2	Hardware du serveur du SC (SerVer HardWare)	serveur
E_S_FWHW	2	Hardware supportant les dispositifs de protection logique de l'entreprise (4.6.1.h) (4.6.3.a) (FireWall HardWare)	serveur
E_L_DWHW	1	Hardware de la machine de développement / qualification / base déploiement (Development Workstation HardWare).	local
E_L_CWHW	1	Hardware des clients du SC (Client Workstation HardWare)	local
E_D_CWHW	0	Hardware des clients du SC (Client Workstation HardWare)	distant
2. - Ressources logicielles		
Ressource	*Confiance*	*Description*	*S/Système*
E_S_SVSW	2	Système d'exploitation et autres logiciels du serveur du SC.	serveur
E_S_FWSW	2	Système d'exploitation et autres logiciels des dispositifs de protection logique de l'entreprise (4.6.1.h) (4.6.3.a)	serveur
E_L_DWSW	1	Logiciels de la machine de développement / qualification / base du déploiement (Système d'exploitation, compilateurs, IDE, etc.)	local
E_L_CWSW	1	Systèmes d'exploitation des clients du SC	local
E_D_CWSW	0	Systèmes d'exploitation des clients du SC	distant
3. - Ressources réseau		
Ressource	*Confiance*	*Description*	*S/Système*
E_S_INET	0	Internet	serveur
E_S_WAN	1	Connexions permanente à l'Internet de l'entreprise (4.6.1.h)	serveur
E_S_LAN	2	Réseau local	serveur
E_L_INET	0	Internet. Confondu avec E_S_INET.	local
E_L_WAN	1	Connexions permanente à l'Internet de l'entreprise (4.6.1.h). Confondue avec E_S_WAN.	serveur
E_L_LAN	1	Réseau local	local
E_D_INET	0	Internet. Confondu avec E_S_INET.	distant
E_D_WAN	1	Connexions non permanente à l'Internet du client, de la filiale ou du télétravailleur.	distant
E_D_LAN	0	Réseau local	distant
4. - Ressources humaines (personnel)		
Ressource	*Confiance*	*Description*	*S/Système*
E_S_ADMIN	2	Administrateur	serveur
E_L_DEV	2	Développeur (utilisateur du poste E_L_DWHW)	local
E_L_USR	1	Utilisateur	local
E_D_USR	0	Utilisateur	distant

[22] Création, modification, suppression, écriture, lecture, transfert et affichage.

Tableau 5.4	**Entités du SC (suite)**	*(localisation sur base des hypothèses en 5.2.4.1)*	
5. - Environnement physique (site)			
Ressource	*Confiance*	*Description*	*S/Système*
E_S_SITE	2	Site d'implantation du serveur (salle fermée et climatisée [5.2.3.4.b])	serveur
E_L_SITE	1	Bureaux de l'entreprise.	local
E_D_SITE	0	Sites clients (variés).	distant
6. - Environnement organisationnel			
Ressource	*Confiance*	*Description*	*S/Système*
E_ENTORG	1	L'entreprise en tant qu'organisation	tous
E_CLIORG	0	Les organisations clientes de l'entreprise	distant

Tableau 5.5	**Représentation des liens fonctions / entités et informations / entités**									
1. - Ressources matérielles										
Fonct. / Inform. Entité	*F_COMM*	*F_ENROL*	*F_DEVEL*	*F_DEPLO*	*I_AUTH*	*I_PROFIL*	*I_COMM*	*I_CODSRC*	*I_CODBIN*	*I_PARAM*
E_S_SVHW	X	X		X	X	X	X		X	X
E_S_FWHW	X			X		X	X			
E_L_DWHW			X	X				X	X	
E_L_CWHW	X			X		X	X		X	
E_D_CWHW	X			X		X	X		X	
2. - Ressources logicielles										
Fonct. / Inform. Entité	*F_COMM*	*F_ENROL*	*F_DEVEL*	*F_DEPLO*	*I_AUTH*	*I_PROFIL*	*I_COMM*	*I_CODSRC*	*I_CODBIN*	*I_PARAM*
E_S_SVSW	X	X		X	X	X	X		X	X
E_S_FWSW	X			X		X	X		X	
E_L_DWSW			X	X				X	X	
E_L_CWSW	X			X		X	X		X	
E_D_CWSW	X			X		X	X		X	
3. - Ressources réseau										
Fonct. / Inform. Entité	*F_COMM*	*F_ENROL*	*F_DEVEL*	*F_DEPLO*	*I_AUTH*	*I_PROFIL*	*I_COMM*	*I_CODSRC*	*I_CODBIN*	*I_PARAM*
E_S_INET	X			X		X	X		X	
E_S_WAN	X			X		X	X		X	
E_S_LAN	X			X		X	X		X	
E_L_INET	X			X		X	X		X	
E_L_WAN	X			X		X	X		X	
E_L_LAN	X		X	X		X	X		X	
E_D_INET	X			X		X	X		X	
E_D_WAN	X			X		X	X		X	
E_D_LAN	X			X		X	X		X	
4. - Ressources humaines										
Fonct. / Inform. Entité	*F_COMM*	*F_ENROL*	*F_DEVEL*	*F_DEPLO*	*I_AUTH*	*I_PROFIL*	*I_COMM*	*I_CODSRC*	*I_CODBIN*	*I_PARAM*
E_S_ADMIN		X		X	X	X			X	X
E_L_DEV			X	X				X	X	
E_L_USR	X	X			X	X	X			
E_D_USR	X	X			X	X	X			
5. - Environnement physique										
Fonct. / Inform. Entité	*F_COMM*	*F_ENROL*	*F_DEVEL*	*F_DEPLO*	*I_AUTH*	*I_PROFIL*	*I_COMM*	*I_CODSRC*	*I_CODBIN*	*I_PARAM*
E_S_SITE	X	X		X	X	X	X		X	X
E_L_SITE	X		X	X		X	X	X	X	
E_D_SITE	X			X		X	X		X	
6. - Environnement organisationnel										
Fonct. / Inform. Entité	*F_COMM*	*F_ENROL*	*F_DEVEL*	*F_DEPLO*	*I_AUTH*	*I_PROFIL*	*I_COMM*	*I_CODSRC*	*I_CODBIN*	*I_PARAM*
E_ENTORG	X	X	X	X	X	X	X	X	X	X
E_CLIORG	X	X					X			

5.3. Etape 2: expression des besoins de sécurité

5.3.1. Présentation de l'étape

L'expression des besoins de sécurité a pour objectif la détermination et l'expression (par exemple en termes de disponibilité[G], d'intégrité[G] et de confidentialité[G]) des besoins de sécurité qui sont associés aux fonctions et catégories d'informations essentielles de la cible de l'étude, ainsi que la quantification de l'impact potentiel sur l'entreprise qu'aurait le non respect de ces besoins. Cette étape est constituée de trois activités:

- la sélection des éléments sensibles,
- la détermination des besoins de sécurité pour chaque élément sensible et
- la synthèse du besoin de sécurité.

La *sélection des événements sensibles* est une démarche qualitative, consistant en pratique à éliminer de la liste des fonctions et catégories d'informations essentielles du SC celles dont la compromission éventuelle (en termes de disponibilité[G], d'intégrité[G] et de confidentialité[G]) n'aurait aucune conséquence pour le SC et l'entreprise.

Appliquée ensuite aux seules fonctions et catégories d'informations sélectionnées (qualifiées comme 'sensibles'), la *détermination des besoins de sécurité* représente l'activité de quantification. Elle établit, pour chaque fonction et catégorie d'information sensible, son besoin en sécurité en s'appuyant sur:

- *(5.3.1.a)* la sélection des critères de sécurité (au minimum, les critères de disponibilité[G], d'intégrité[G] et de confidentialité[G], mais d'autres sont envisageables);
- *(5.3.1.b)* l'établissement d'une échelle de sensibilité (voir tableau 5.6);
- *(5.3.1.c)* l'identification d'un certain nombre de sinistres types pour chaque critère de sécurité (liste de sinistres qui diffère selon que l'on considère une fonction ou une catégorie d'informations essentielle);
- *(5.3.1.d)* la sélection (sur base d'une liste non exhaustive de propositions) des types d'impacts probables sur l'entreprise en fonction de la liste des sinistres établie.

Tableau 5.6	**Echelle des sensibilités** (source: [EB-T])
Sensibilité	*Description*
0	Le sinistre ne risque pas de provoquer une gêne notable dans le fonctionnement ou les capacités à court et long terme de l'entreprise.
1	Susceptible (avec une probabilité supérieure à 30% si l'atteinte se produit), de provoquer une gêne dans le fonctionnement de l'entreprise, cette gêne pouvant elle-même provoquer une diminution des capacités de l'entreprise.
2	Susceptible d'amoindrir notablement les capacités de l'entreprise (avec une probabilité supérieure à 30% si l'événement se produit), avec pertes financières et/ou sanctions administratives à plus ou moins longue échéance.
3	Susceptible de provoquer, avec une probabilité supérieure à 20 % si l'atteinte se produit, une modification importante dans les structures et la capacité de l'entreprise (restructuration et/ou révocation de dirigeants).
4	Susceptible de mettre en cause, avec une probabilité supérieure à 20%, la pérennité de l'entreprise considérée.

Cette démarche de *détermination des besoins de sécurité*, matérialisée par l'établissement d'une *fiche d'expression des besoins de sécurité* pour chaque fonction et catégorie d'information sensible, peut être illustrée par le pseudo code de la figure 5.4 page suivante. En pratique, EBIOS préconise que les fiches vierges d'évaluation soient établies et distribuées à chaque utilisateur concerné. Une fois les fiches remplies (et les évaluations motivées), l'évaluateur (5.1.5.a) établit la *synthèse des besoins de sécurité* (dernière activité de l'étape).

```
début traitement
        pour chaque élément essentiel (fonction ou information):
        début élément essentiel
                création d'une nouvelle fiche
                pour chaque critère (disponibilité, intégrité, confidentialité, autre(s)):
                début critère
                        pour chaque sinistre affectant ce critère pour ce type d'élément essentiel (fonction ou
                        information):
                        début sinistre
                                pour chaque type d'impact
                                début type d'impact:
                                        évaluation de l'impact (selon l'échelle d'évaluation établie)
                                fin type d'impact
                                détermination de l'impact maximum (selon l'échelle d'évaluation établie)
                        fin sinistre
                fin critère
                validation de la fiche
        fin élément essentiel
fin traitement
```

Figure 5.4: algorithme d'établissement des fiches d'expression des besoins de sécurité. Des exemples de ces fiches figurent en ANNEXE 2.

5.3.2. Etape 2 - Activité 1: sélection des éléments sensibles

La sensibilité d'une catégorie d'information résulte de la valeur que nous attribuons à ces informations: s'agit-il d'un secret défense ou d'un patrimoine onéreux à reconstituer, les critères d'appréciation ne manquent pas, au point qu'une des méthodes inspirées de la technique 2.1-A [EB-T] du guide EBIOS pourrait simplement consister à écarter les catégories d'informations non sensibles, c'est-à-dire celles dont la perte, la divulgation ou l'altération n'aurait aucune conséquence.

De ce dernier point de vue, toutes nos catégories d'informations paraissent sensibles, comme indiqué par le tableau 5.7.

Tableau 5.7	**Liste des catégories d'informations sensibles**
Catégories (5.2.3.3.)	*Motivation*
I_AUTH	Si l'identification est requise (3.1.c), il paraît logique d'imaginer que la perte, la divulgation ou l'altération de cette catégorie d'informations ne serait pas sans conséquence (4.5.2).
I_PROFIL	Sans chercher très loin, rien que l'identité (5.2.3.3.f) des clients est déjà confidentielle (4.4.2.d).
I_COMM	Le contenu des conversations constitue une catégorie d'informations sensible (4.4.2.e).
I_CODSRC	Le code source, surtout en phase de développement, est une catégorie d'information sensible (4.7.2.a).
I_CODBIN	C'est le code binaire qui paraît constituer la catégorie d'information la moins sensible (4.7.2.e). Nous la retiendrons malgré tout, non pas parce qu'une atteinte à son intégrité nous obligerait à redéployer l'application, mais à cause de la contribution négative que cela aurait[23], en décourageant l'utilisateur, par rapport à notre objectif d'amélioration du support (2.1.3.b).
I_PARAM	Une altération des paramètres de configuration du SC ne serait sûrement pas sans conséquences[24].

La question est plus aisée encore en ce qui concerne les fonctions du système: qu'une seule d'entre elles ne soit plus conforme[G] - ou même simplement plus disponible[G] - et l'ensemble du système risque de devenir, dans le meilleur des cas et à plus ou moins brève échéance, indisponible. Nous considérerons donc que toutes les fonctions essentielles du système sont sensibles.

[23] L'impact ressenti le serait au niveau de la disponibilité[G].

[24] Inversement, nous pourrions poser que si une telle altération n'avait aucune conséquence, la raison d'être de ces paramètres serait difficile à trouver.

Le fait que toutes les fonctions et catégories d'informations soient considérées comme sensibles peut nous interpeller quant au rôle et à l'utilité de cette sélection. Il convient toutefois de se rappeler que EBIOS a été conçue pour permettre la réalisation d'études de sécurité de SC bien plus étoffées que la nôtre, par exemple constituées de plusieurs applications distinctes constituant tout ou partie du SI d'une entreprise.

5.3.3. Etape 2 - Activité 2: expression du besoin de sécurité

Pour pouvoir exprimer le besoin de sécurité nous avons vu (5.3.1) qu'il nous fallait au préalable définir:

- nos critères de sécurité (5.3.1.a),
- une échelle d'évaluation de la sensibilité selon ces critères (5.3.1.b),
- les types de sinistres craints (5.3.1.c) et
- les impacts possibles (5.3.1.d).

Les *critères de sécurité* que nous utiliserons sont les critères traditionnels de disponibilité[G], d'intégrité[G], de confidentialité[G] et d'imputabilité[G], auxquels sans surprise nous ajouterons notre critère d'écologie[G]. Cette liste correspond à celle que nous avions arrêtée au début du chapitre précédent (Objets et critères de sécurité (4.2)).

Nous adopterons également l'*échelle de sensibilité* proposée par la méthode EBIOS (tableau 5.6). Chaque fois qu'un des sinistres envisagés pour une fonction ou une catégorie d'informations produira ses effets sur le SC suivant un cas de figure correspondant à un de ceux évoqués au chapitre précédent (dans lequel nous considérions le SC dans son ensemble), nous transposerons notre évaluation antérieure vers l'échelle EBIOS selon le tableau de correspondance reproduit ci-dessous (tableau 5.8) *(5.3.3.a)*. Notons que comme nous l'avions fait au chapitre précédent, EBIOS préconise que l'évaluation de l'impact ne tienne pas compte ici de la probabilité réelle de survenance du sinistre *(5.3.3.b)*.

Tableau 5.8 | **Correspondance entre échelles d'évaluation**			
Echelle proposée par EBIOS (tableau 5.6) pour application, par critère, aux fonctions et catégories d'informations essentielles du SC		*Notre échelle du chapitre 4 (4.2) telle qu'appliquée, par critère, au SC tout entier.*	
Pas de gêne notable.	0	0	Non significatif (impact marginal)
Gêne possible.	1	0	Non significatif (impact marginal)
Gêne probable avec pertes financières et/ou sanctions administratives.	2	1	Significatif (effort pour assumer)
Risque de modification importante dans les structures et la capacité de l'entreprise.	3	2	Grave (remise en cause des objectifs)
Risque pour la pérennité de l'entreprise.	4	3	Catastrophique (atteinte à la pérennité)

Issus tantôt du guide EBIOS (technique 2.1-B [EB-T]), tantôt du chapitre précédent, les *types de sinistres* plausibles sont repris au tableau 5.9 à la page 54. Le lecteur y retrouvera:

- une colonne avec les types de sinistres proposés par la méthode EBIOS, colonne dans laquelle nous avons ajouté en *caractères italiques* quelques types issus de notre réflexion du chapitre précédent, et
- une autre colonne permettant d'établir un lien avec ce même chapitre précédent.

Ce tableau, établi sur base de certaines hypothèses supplémentaires, mérite les quelques commentaires qui suivent (au niveau des fonctions d'abord, des catégories d'informations ensuite):

- *(5.3.3.c)* lorsque nous avons abordé le critère de disponibilité[G] au chapitre précédent(4.3), nous n'avons pas réellement envisagé l'impact de l'*indisponibilité complète de longue durée* (EBIOS), que nous assimilerons ici au non-respect du SLA proposé (4.3.3). Comme ce genre d'indisponibilité, susceptible de nous pousser à l'abandon pur et simple du système, nous paraît dans certains cas moins préjudiciable à moyen et long terme que celle d'un système où les problèmes - et l'insatisfaction - seraient récurrents, nous pourrons parfois transposer les valeurs du tableau 4.1 à ce type d'indisponibilité fonctionnelle;
- *(5.3.3.d)* lorsque certains utilisateurs n'ont pas accès au système, nous considérerons qu'il s'agit d'une *indisponibilité complète de courte durée* (sensu EBIOS). Indisponibilité complète, c'est assurément le cas pour les personnes empêchées, mais aussi et indirectement pour d'autres si la

personne empêchée est le préposé au support. Quant à affirmer qu'elle est de *courte durée*, il s'agit là d'une hypothèse gratuite concernant les capacités d'intervention du personnel de l'entreprise;

- *(5.3.3.e)* nous considérons la *dégradation de performance* (disponibilité[G]) dans le cas pire, c'est-à-dire comme une conséquence d'un phénomène structurel (persistant) et non conjoncturel (temporaire) (4.3.3.d);
- *(5.3.3.f)* les besoins de confidentialité[G] par rapport à l'existence du projet (4.4.1.a) et de l'application (4.4.1.b) n'ayant pas été retenus au chapitre précédent (4.4.2.a) (4.4.2.b), nous ne tiendrons plus compte de ce critère en ce qui concerne les fonctions;
- *(5.3.3.g)* conformément à notre discussion sur la pertinence du critère d'imputabilité[G] (4.5.1) dans notre application, nous envisagerons ce critère sous l'angle unique de la question générale du *qui*[25]. Nous considérerons donc qu'il y aura atteinte à ce critère en cas d'usurpation d'identité;
- *(5.3.3.h)* à notre entendement, le concept EBIOS d'*intégrité*[G] *d'une fonction* est davantage porteur de sens dans le contexte d'un SI composé de multiples fonctions, dont certaines peuvent être organisationnelles ou procédurales, que dans le cas de notre SC. Nous ne retiendrons donc pas ce critère pour notre évaluation des fonctions;
- *(5.3.3.i)* l'écologie[G], qui est davantage une question de comportement que d'état, s'avère un critère relevant des seules fonctions du SC[26][27]. Pour l'analyse de ce critère, nous ne tiendrons pas compte des postes clients (voir figure 5.3) (4.6.1.b) puisque nous ne pouvons pas connaître a priori leur type ni n'avons de moyen d'action sur la plupart d'entre eux (raison pour laquelle, au tableau 5.4, certains se sont vu attribuer un niveau de confiance égal à 0).
- *(5.3.3.j)* nous n'avions pas approché la confidentialité[G] au chapitre précédent sous l'angle de vue de l'étendue de la divulgation (interne ou externe). Nous parlerons de divulgation interne lorsque celle-ci ne dépasse pas le cadre des employés de l'entreprise, et de divulgation externe dans le cas contraire;
- *(5.3.3.k)* nous considérons une organisation du développement dans laquelle le déploiement n'est possible que pour du code dûment validé.
- *(5.3.3.l)* au chapitre précédent, nous n'avions pas envisagé le problème de la disponibilité[G] sous l'angle des informations, considérant implicitement, vu la taille réduite du système, que l'indisponibilité des informations impliquait celle du SC lui-même;
- *(5.3.3.m)* le critère d'imputabilité[G] pour une catégorie d'informations correspond habituellement à celui d'imputabilité[G] pour la fonction du SC qui l'a générée; nous parlerons alors d'*usurpation d'identité d'un utilisateur* (E_L_USR). Lorsque ce ne sera pas le cas, cela suppose l'intervention d'éléments externes au SC (accès logique ou physique aux machines ou aux réseaux): nous parlerons alors d'*usurpation des privilèges de l'administrateur* (5.2.4.2.b) (E_S_ADMIN) ou d'*usurpation des privilèges d'un développeur* (E_L_DEV);
- *(5.3.3.n)* au chapitre précédent, nous n'avions pas fait de distinction entre atteinte *volontaire* (qui suppose une volonté de nuire) et *accidentelle* à l'intégrité des données, considérant chaque fois le cas pire. Dans certains cas cette distinction ne se justifie peut-être pas (I_CODBIN, par exemple), mais dans d'autres (I_CODSRC, I_AUTH, ...) elle s'avère tout à fait relevante.

Les *impacts possibles*, quant à eux, ont déjà été sélectionnés puisqu'ils correspondent à autant de situations d'échec par rapport aux objets de la protection tels que définis au début du chapitre précédent (4.2: Objets et critères de sécurité).

Il ne nous reste plus à ce stade qu'à établir une fiche par fonction et par catégorie d'informations, puis de les reproduire en autant d'exemplaires qu'il y a de personnes (utilisateurs, techniciens, etc.) concernés par le SC (dans notre cas, un seul exemplaire que nous remplirons en tant qu'administrateur). Le lecteur trouvera le détail de ces fiches en ANNEXE 2.

[25] Validité des informations utilisées par les routines d'mputation du SC.

[26] Il s'agit ici d'une forme de simplification, puisque nous pourrions tout aussi bien considérer qu'une atteinte à l'intégrité de certains paramètres de configuration (I_PARAM) pourrait avoir un impact au niveau de l'écologie de l'application.

[27] Pour rappel, une atteinte (un sinistre par rapport) à la propriété d'écologie[G] de notre application produit un impact sur les autres applications; selon ce critère, c'est donc bien de cet impact sur les autres applications que nous estimerons l'importance.

Tableau 5.9		**Types de sinistres plausibles**	
Cible affectée	*Critère*	*Types de sinistres (EBIOS et ajouts)*	*Types de sinistres (notre chapitre 4)*
Fonctions	Disponibilité	Interruption complète (longue durée) de la fonction (5.3.3.c).	- non respect du SLA défini en (4.3.3)
		Interruption complète (courte durée) de la fonction (5.3.3.d).	- le SC ne fonctionne *provisoirement* (4.3.2.a) pas (4.3.1.a) - tous les utilisateurs n'ont pas accès au SC (4.3.1.b) - absence d'interlocuteur (4.3.1.c)
		Dégradation persistante (5.3.3.e) des performances.	- mauvaises performances (4.3.1.d)
	Confidentialité (5.3.3.f)	Divulgation de l'existence de la fonction.	- en tant que projet (4.4.1.a) - en tant qu'application en production (4.4.1.b)
		Divulgation de l'algorithme de la fonction.	- confidentialité du code source (4.4.1.c)
	Imputabilité (5.3.3.g)	*Usurpation de l'identité d'un utilisateur* (5.3.3.m); *Usurpation des privilèges de l'administrateur* (5.3.3.m); *Usurpation des privilèges d'un développeur* (5.3.3.m)	- usurpation d'identité (4.5.1.f)
	Ecologie (5.3.3.i)	*Incompatibilité entre applications*	- rapports entre le SC et les autres applications (4.6.1.b)
		Saturation des ressources	- rapports entre le SC et son environnement (4.6.1.c)
	Intégrité (5.3.3.h)	Résultats incorrects.	
		Résultats incomplets.	
Informations	Disponibilité (5.3.3.l)	Perte totale (destruction) de l'information.	
		Perte temporaire (inaccessibilité) de l'information.	
	Confidentialité	Divulgation interne (5.3.3.j).	- confidentialité des données (4.4.1.d) (4.4.1.e) (4.4.1.f) (4.4.1.g) (4.4.1.h)
		Divulgation externe (5.3.3.j).	- confidentialité des données (4.4.1.d) (4.4.1.e) (4.4.1.f) (4.4.1.g) (4.4.1.h)
	Imputabilité (5.3.3.g)	*Usurpation de l'identité d'un utilisateur* (5.3.3.m); *Usurpation des privilèges de l'administrateur* (5.3.3.m); *Usurpation des privilèges d'un développeur* (5.3.3.m)	- usurpation d'identité (4.5.1.f)
	Intégrité (5.3.3.n)	Modification accidentelle.	- Intégrité des codes (source et binaire) (4.7.1.a) et des données (4.7.1.b) (4.7.1.c) (4.7.1.d) (4.7.1.e)
		Modification délibérée.	- Intégrité des codes (source et binaire) (4.7.1.a) et des données (4.7.1.b) (4.7.1.c) (4.7.1.d) (4.7.1.e)

5.3.4. Etape 2 - Activité 3: synthèse du besoin de sécurité

La fiche de synthèse des besoins de sécurité, élaborée sur base des expressions individuelles de ces besoins (ANNEXE 2, tableaux A2.1 à A2.10), est illustrée par le tableau 5.10 page suivante.

Tableau 5.10		**Fiche de synthèse d'expression des besoins de sécurité**						
		Profils utilisateurs						
Cible affectée	*Critères*	*Utilisat. clients*	*Utilisat. employés*	*Adminis. SC*	*Dévelop.*	*Utilisateurs Commerciaux*	*MAX*	*Commentaires éventuels*
F_COMM	Disponibilité			2			2	
	Imputabilité			3			3	
	Ecologie			4			4	Configuration: 4 Ressources: 3
F_ENROL	Disponibilité			1			1	
	Imputabilité			3			3	
	Ecologie			2			2	
F_DEVEL	Disponibilité			1			1	
	Imputabilité			3			3	
	Ecologie			2			2	
F_DEPLO	Disponibilité			1			1	
	Imputabilité			0			0	
	Ecologie			4			4	Configuration: 4 Ressources: 3
I_AUTH	Disponibilité			2			2	
	Confidentialité			3			3	Divulgation externe (5.3.3.j)
	Imputabilité			3			3	
	Intégrité			3			3	
I_PROFIL	Disponibilité			2			2	
	Confidentialité			2			2	Divulgation externe (5.3.3.j)
	Imputabilité			2			2	
	Intégrité			2			2	
I_COMM	Disponibilité			2			2	
	Confidentialité			3			3	
	Imputabilité			3			3	
	Intégrité			2			2	
I_CODSRC	Disponibilité			2			2	Perte totale (destruction)
	Confidentialité			0			0	
	Imputabilité			3			3	
	Intégrité			3			3	
I_CODBIN	Disponibilité			2			2	
	Confidentialité			0			0	
	Imputabilité			2			2	
	Intégrité			2			2	
I_PARAM	Disponibilité			2			2	
	Confidentialité			0			0	
	Imputabilité			3			3	
	Intégrité			3			3	

5.4. Conclusions

5.4.1. Evaluation de l'approche EBIOS

L'approche EBIOS ne prévoit pas vraiment une évaluation à ce stade de la démarche, le document final (tableau 5.10) étant destiné à devenir la matière première pour une étape ultérieure. Il nous apparaît utile, néanmoins, de prendre ici un peu de recul pour analyser a posteriori la démarche suivie et les résultats obtenus.

Au niveau de la démarche, si celle-ci apparaît de prime abord comme simple, raisonnablement structurée et facile à mettre en oeuvre, nous avons néanmoins rencontré un certain nombre de difficultés lors de la définition du SC et de l'établissement des critères et fiches d'expression des besoins de sécurité.

La définition du SC (deuxième activité de la première étape (5.2.3)) constitue une opération importante dont les deux moments forts sont probablement la définition du SC par rapport au SI de l'entreprise et la représentation fonctionnelle du SC.

La demande de *définition du SC par rapport au SI de l'entreprise* (5.2.3.1) (5.2.3.2) nous a quelque peu surpris dans la mesure où nulle part auparavant EBIOS ne nous avait encore invités à définir les objectifs du SC comme nous l'avions fait au chapitre 3 (fin de la première partie). Il nous faut, à notre avis, en trouver l'explication dans le fait qu'EBIOS est une méthode dont l'objectif est l'évaluation des besoins de sécurité et de sécurité

seulement; à ce titre, indépendante du choix du cycle de vie du produit, elle vient en complément et non en remplacement d'une démarche ou méthode de définition des objectifs et exigences fonctionnelles. Cette indépendance est intéressante, mais elle a un prix: celui d'un couplage relativement faible entre les exigences des domaines fonctionnels et celles liées aux considérations de sécurité, et donc d'une moins bonne traçabilité globale de l'évolution des besoins en exigences et spécifications *(5.4.1.a)*.

Par la suite, la multiplication des hypothèses que nous avons été contraints de poser nous a conforté dans notre idée concernant la nécessité d'une démarche préalable de description fonctionnelle[28] de notre application.

Pour ce qui est de la *représentation fonctionnelle du SC*, l'opération la plus délicate fut sans nul doute le choix du bon niveau de représentation. A ce stade de la démarche, ce qui nous intéresse sont les fonctions et

informations qui interagissent directement avec le reste du SI de l'entreprise (celles qui sont perceptibles en vue externe du SC), et non les fonctions et informations du SC lui-même telles qu'introduites par le chapitre 3 susmentionné. Pour être initialement tombés dans ce piège, nous nous sommes rendus compte de l'impasse à laquelle cela nous menait dès lors qu'il a été question, par la suite, d'établir les fiches d'expression des besoins de sécurité[29].

Malgré la diminution du nombre de fonctions et catégories d'informations essentielles à laquelle nous avons alors procédé, *l'établissement des critères et fiches d'expression des besoins de sécurité* s'est néanmoins encore avéré une opération très délicate, comme l'indique le nombre de commentaires et d'hypothèses préalables en (5.3.3). A notre sens, beaucoup de ces hypothèses sont discutables, et cela introduit une certaine incertitude quant au résultat final. Par la suite, lors de l'évaluation sur fiches des critères sélectionnés, nous avons souvent été confrontés à des réflexions byzantines sur des questions de causalité: par exemple, si nous envisageons le cas de figure d'une fonction essentielle qui s'avérerait non conforme[G], devons-nous en imputer l'impact au critère d'intégrité[G] des fonctions essentielles (que nous avions décidé de ne pas considérer (5.3.3.h)), au critère d'intégrité[G] du code de l'application (source ou binaire ?) ou à celui d'imputabilité[G] (usurpation de l'identité du développeur)[30] ? Ou encore, lorsqu'une divulgation résulte d'une usurpation d'identité, faut-il en attribuer l'impact à la confidentialité[G], à l'imputabilité[G] ou aux deux ? Toutes questions auxquelles, la plupart du temps, nous avons tenté de répondre en considérant les situations de la manière la plus large possible, c'est-à-dire en distribuant généreusement les impacts estimés pour un même type de sinistre sur plusieurs critères *(5.4.1.b)*.

De même, le simple fait de sortir des trois critères principaux que sont la disponibilité[G], l'intégrité[G] et la confidentialité[G] complique singulièrement la tâche pour qui devrait, en distribuant les fiches, expliquer aux personnes concernées ce que signifie l'imputabilité[G] telle que nous l'avons réduite au problème d'usurpation d'identité (4.5.1), ou l'écologie[G] selon la définition de laquelle une atteinte à cette propriété du SC produirait ses effets sur une autre partie du SI (élément du SI externe au SC, ou autre fonction / type d'information essentielle du SC) avec un impact à évaluer, par exemple, sur les objectifs stratégiques de l'entreprise.

On le voit, la démarche d'établissement des besoins de sécurité via les fiches établies ne s'apparente pas vraiment à une science exacte[31]. Notre opinion est que la validité du résultat final sera directement proportionnelle au nombre de personnes concernées qui auront contribué à l'élaborer et que, l'un dans l'autre, les différentes perceptions et sensibilités qui auront pu s'exprimer en seront les garantes. Ce qui nous incite à considérer avec prudence les résultats obtenus suite à notre démarche solitaire *(5.4.1.c)*.

5.4.2. Résultats de l'approche EBIOS

Une interprétation quantitative (basée par exemple sur le nombre de fois qu'un critère est cité à une certaine valeur d'impact) des résultats intermédiaires de l'approche EBIOS nous paraissant par trop dépendante du

[28] A ne pas confondre avec la démarche EBIOS de *représentation fonctionnelle* (5.2.3.3).

[29] La granularité trop fine (au niveau de la définition des fonctions et catégories d'informations essentielles) et la trop grande proximité du technique par rapport au fonctionnel nous avaient poussés à devoir envisager un nombre important de questions sans objet, voire insolubles.

[30] Une autre manière de tourner la question consisterait à se demander si du code source doit être assimilé à une information (notre hypothèse), ou à une fonction (ce qui donnerait davantage de sens au concept d'intégrité de fonction lorsque cette dernière est une fonction informatisée (5.3.3.h)).

[31] Notre démarche du chapitre précédent n'échappe pas davantage à cette critique.

nombre de fonctions et catégories d'informations essentielles identifiées dans le SC (5.2.3.3) et considérées comme sensibles (5.3.2), nous nous limiterons à une prudente observation qualitative, illustrée par le tableau 5.11, et d'où il ressort que:

- l'écologie[G] est le seul critère qui puisse provoquer un impact de niveau 4 de l'échelle EBIOS;
- imputabilité[G], confidentialité[G] et intégrité[G] occupent la plage médiane (niveaux 2 et 3);
- la disponibilité[G] n'apparaît qu'au niveau 2 et est le seul critère représenté au niveau 1 de l'échelle EBIOS.

Tableau 5.11	**Niveaux d'impacts atteints par critère**			
Echelle EBIOS: / *Critères:*	*1*	*2*	*3*	*4*
Ecologie				
Imputabilité				
Confidentialité				
Intégrité				
Disponibilité				

Le partage de la plage médiane par les trois critères d'imputabilité[G], de confidentialité[G] et d'intégrité[G] s'explique probablement par la difficulté déjà mentionnée qu'il y a à faire ressortir les causalités exactes lorsque plusieurs critères sont susceptibles de s'imbriquer (5.4.1.b). Clairement, si nous devions recommencer cette évaluation, c'est à ce niveau que se porteraient nos efforts d'affinement.

5.4.3. Comparaison des approches

Nous avons également souhaité établir une comparaison rapide entre les démarches et résultats des deux chapitres d'évaluation des besoins de sécurité, comparaison dont le but est avant tout de mieux approcher le niveau de confiance que nous pouvons accorder aux résultats obtenus.

L'impression générale que nous retiendrons de cette double approche est qu'une méthode induit plus de structure, et que la structure permet une plus grande complétude. A contrario, nous dirions que par rapport à une démarche sans a priori, le respect strict d'une structure imposée pourrait parfois, d'une part, mener à des considérations qui ne seraient pas toujours porteuses de sens, et d'autre part s'avérer un élément relativement réducteur par le canevas dans lequel il risque d'enfermer la réflexion.

Ces considérations mises à part, la principale différence entre les deux approches se situe au niveau de l'algorithme utilisé. Au chapitre 4 nous sommes partis des critères, et pour chacun d'entre eux nous avons tenté d'évaluer l'impact d'un sinistre affectant ce critère par rapport à un certain nombre d'éléments qu'a posteriori nous qualifierions de sensibles (toujours par rapport à ce critère). La sélection de ces éléments s'est donc opérée naturellement, selon leur pertinence par rapport au critère étudié, avec ce que cela aura pu impliquer comme oublis ou incohérences, et le résultat de la démarche est une évaluation par critère. Dans ce chapitre 5, la démarche fut inverse: pour chaque élément du SC identifié et estimé sensible, les différents critères d'évaluation de la sécurité ont été passés en revue et l'impact évalué[32] - avec comme résultat une quantification de la sensibilité des éléments en question.

Fondamentalement, notre approche intuitive ne s'appuyait donc sur aucune définition préalable des éléments sensibles, ce qui a pu induire parfois un certain manque de rigueur - voire de cohérence - mais qui, d'autre part, nous a permis de fonctionner sans avoir à poser autant d'hypothèses préalables sur l'architecture[33], et sans même ressentir le besoin de la définition fonctionnelle préalable que constitue le chapitre 3[34].

Mais au-delà de ces différences, il nous plaît aussi de constater l'existence d'un certain nombre de convergences que nous résumerons rapidement dans les quelques lignes qui suivent:

- la démarche générale est identique: elle consiste à présenter d'abord l'entreprise et le contexte, puis le projet (en termes d'objectifs ou de définition fonctionnelle), et enfin à établir les besoins de sécurité;
- les outils d'analyse (critères et échelles d'évaluation) sont identiques ou comparables;
- nous pourrions même parler de similitude du méta modèle, lequel pourrait être représenté sous la forme d'un diagramme de classes exprimant les informations suivantes:

[32] Pour autant que le critère ait été jugé pertinent par rapport à l'élément ou au type d'élément sensible.
[33] Il n'est toutefois pas douteux que certaines hypothèses implicites aient pu y jouer un rôle.
[34] Le chapitre 3 a été inséré en fin de première partie pour les besoins de la méthode EBIOS, alors que la première version du chapitre 4 était déjà couchée sur papier.

- les menaces[G] *exploitent* des vulnérabilités[G] en *causant* des sinistres
- les sinistres *provoquent* des impacts
- l'auditeur *utilise* une échelle pour *évaluer* un impact *selon* certains critères

Tenant compte de ces similitudes, auxquelles s'ajoute l'unicité de l'évaluateur et de certaines de ses évaluations (utilisées dans les deux chapitres), nous nous attendions à ce que les deux démarches produisent des résultats comparables. La forme sous laquelle ces résultats se présentent n'en facilite pas la comparaison, mais celle-ci reste néanmoins possible: si nous regroupons dans un seul et même tableau le contenu du tableau 5.11 et celui du tableau 4.7[35], cela nous donne le tableau 5.12 que voici:

Tableau 5.12	**Niveaux d'impacts atteints par critère** (tableau comparatif)				
Echelle EBIOS:	*(tab. 5.7)*	*1*	*2*	*3*	*4*
Notre échelle:	*(tab. 5.9)*	*0*	*1*	*2*	*3*
Critères:					
Ecologie					
	EBIOS				
	(tab. 4.7)				
Imputabilité					
	(EBIOS				
	(tab. 4.7)				
Confidentialité					
	EBIOS				
	(tab. 4.7)				
Intégrité					
	EBIOS				
	(tab. 4.7)				
Disponibilité					
	EBIOS				
	(tab. 4.7)				

Pour conclure, nous dirions qu'il nous paraît difficilement envisageable d'effectuer un travail sérieux d'expression des besoins de sécurité sans utiliser une méthode aidant à structurer la pensée, mais que cet outil quel qu'il soit ne devrait jamais nous dispenser d'une démarche préalable de réflexion libre d'a priori. D'autres types de méthodes empruntent par ailleurs cette approche, méthodes qui commencent explicitement par un *brainstorming* avant d'entamer toute phase plus structurée[36].

[35] Tableau qui comprend la synthèse des impacts évalués au chapitre 4 avant la pondération selon notre idée de la probabilité réelle de survenance, ce qui fait de ce tableau le pendant exact du tableau 5.11 (5.3.3.b).

[36] Par exemple la *Risk Assement Method*, dont le lecteur trouvera une brève description dans [Erwin-00]. Dans cet article, extrait d'un livre du même auteur, le principe du brainstorming est utilisé jusqu'à l'identification des risques.

Troisième partie Identification des menaces

Après avoir qualifié nos besoins principaux en matière de sécurité (chapitres 4 et 5), nous allons tenter d'identifier la nature des menaces[G] à prendre en considération.

Chapitre 6 Approche statistique

Que pouvons nous tirer comme enseignement de la sinistralité informatique recensée ?

6.1. Principe

Le principe de cette première approche est extrêmement simple, voire simpliste: il consiste, sur base des statistiques des sinistres informatiques, à tenter de cerner la nature des menaces[G] les plus importantes. L'idée sous-jacente consiste à penser, par exemple, que si la disponibilité[G] ne représente pas un critère de sécurité important pour notre application (4.8.h), il n'est peut-être pas besoin d'investir dans des mesures de prévention ou de protection par rapport aux causes identifiées des types de sinistres recensés ayant eu un impact sur ce seul critère.

Notre intention dans ce chapitre est donc d'expérimenter une démarche d'identification des menaces[G] basée sur des données statistiques existantes en procédant comme suit:

- pour chaque critère d'évaluation:
  - déterminer les menaces[G] responsables d'une *majorité importante*[37] des sinistres recensés: nous avons choisi, arbitrairement, de fixer le seuil aux environs du percentile 85;
  - des menaces[G] identifiées, éliminer celles qui ne seraient pas relevantes[38] [39] (en général, ou par rapport au critère évalué);
- et pour terminer, tenter une pondération des menaces[G] résiduelles, pondération qui tienne compte entre autres de l'expression de nos besoins de sécurité.

6.2. Types de menaces

6.2.1. Nécessité d'une nomenclature

Pour ce faire, nous avons besoin de regrouper en catégories les différentes causes possibles des sinistres informatiques, ce qui permet d'effectuer des comparaisons et d'observer des corrélations éventuelles entre types de causes[40] et types de conséquences[41]. Une approche fréquemment utilisée consiste à tirer parti de la

[37] L'unité de mesure utilisée (fréquence des sinistres, importance des impacts) dépendra des données disponibles.
[38] Par exemple, la menace[G] que représenterait un tremblement de terre pourrait être considérée comme non relevante dans une région géologiquement stable.
[39] Une menace non prise en considération pour manque de relevance sera considérée comme *traitée* et ne remettra pas en cause la valeur du percentile.
[40] La *cause d'un sinistre* est une menace[G] qui aurait conduit à une violation effective de la sécurité; comme il n'est question dans ce chapitre que des seules menaces[G] devenues *causes de sinistres*, nous utiliserons indifféremment l'une ou l'autre expression.
[41] Chaque *type de conséquence* exprime un impact sur un critère comme la disponibilité[G], la confidentialité[G], l'intégrité[G] ou l'imputabilité[G].

grille harmonisée des menaces[G] [42] *informatiques* établie par le *Comité Européen des Assurances* ou CEA [CEA].

6.2.2. Les types de menaces selon le CEA

La *grille harmonisée des menaces*[G] *informatiques* établie par le CEA [CEA] identifie treize types de menaces[G] répartis en trois catégories: les accidents ('A'), les erreurs ('E') et les actes de malveillance ('M') (tableau 6.1.). Cette grille est reprise avec davantage de détails en ANNEXE 4.

Tableau 6.1.	**Les 3 catégories et 13 types de menaces**
Catégories et Types de menaces	*Description*
Catégorie 'A'	*Accidents*
A1 Physiques	Incendie, explosion, implosion.
A2 Pannes	Pannes matérielles et logicielles (causes d'origine ou de révélation interne).
A3 Evénements naturels (force majeure)	Ensemble des événements naturels d'origine externe comme par exemple inondation, tempête, ouragan, grêle, poids de la neige, avalanche, coulée de boue, glissement de terrain, phénomènes sismiques ou volcaniques, etc.
A4 Perte de services essentiels	Causes d'origine externe entraînant le dysfonctionnement: coupure d'alimentation électrique ou des télécommunications, rupture de stock en fournitures ou pièces essentielles, etc.
A5 Autres	Autres causes physiques: chocs, chutes, pollution chimique ou par rayonnement, etc.
Catégorie 'E'	*Erreurs*
E1 Erreurs d'utilisation	Erreurs d'utilisation (logiques): de saisie ou de transmission de données, d'exploitation du système.
E2 Erreurs de conception	Erreurs de conception ou de réalisation des logiciels et des procédures d'exploitation
Catégorie 'M'	*Malveillance*
M1 Vol	Vol de matériels principaux ou accessoires.
M2 Fraude	Utilisation non autorisée des ressources du système conduisant à un préjudice évaluable monétairement, essentiellement formé par le détournement de fonds, de biens ou de services.
M3 Sabotage	Action malveillante conduisant à un sinistre matériel de type A1 ou A2.
M4 Attaque logique	Utilisation non autorisée des ressources du système conduisant à un préjudice au moins qualitatif (souvent une perte de disponibilité ou d'intégrité) et entraînant souvent un profit indirect pour l'auteur des faits.
M5 Divulgation	Utilisation non autorisée des ressources du système entraînant la divulgation à des tiers d'informations confidentielles.
M6 Autres	Grèves, perte ou indisponibilité de personnel, contrefaçon de progiciels, etc.

6.3. Données statistiques utilisées

6.3.1. Le CLUSIF

Le *Club de la Sécurité Informatique Français* (CLUSIF) a contribué à mettre en place un observatoire de la sinistralité des menaces[G] informatiques dans le but d'en évaluer l'impact économique et son évolution dans le temps. Nous avons choisi, pour notre tentative d'approche statistique, d'utiliser leurs données pour les raisons suivantes:

- le CLUSIF utilise la grille d'évaluation du CEA;
- la sinistralité y est ventilée en fonction du critère atteint (disponibilité[G], intégrité[G], confidentialité[G])[43];
- il s'est avéré très difficile de trouver d'autres statistiques qui soient fiables et utilisables.

[42] L'appellation exacte est *grille harmonisée des risques informatiques*. Nous avons préféré, par souci de cohérence, substituer le terme *menace*[G] au terme *risque*[G].
[43] Le CLUSIF parle dans ce cas de ventilation par conséquences *primaires* ou *directes*.

6.3.2. Les rapports de 1991 à 1996

Ces 6 rapports annuels [CLUSIF19] ont été établis à méthodologie relativement constante (de légères variations existent) sur base des sinistres (informatique, bureautique et télécoms) connus et déclarés *en France pour le secteur non gouvernemental (6.3.2.a)* au cours de l'année antérieure. Ils expriment les pertes financières[44] (pertes matérielles et pertes d'exploitation, en millions de francs français) estimées au plus tard dans les trois mois du sinistre pour une période de 12 mois consécutifs au sinistre. Ces estimations, de l'avis même des rapporteurs, sont à considérer avec une marge d'erreur proche de 30% *(6.3.2.b)*.

6.3.3. Les rapports de 2000 et 2001

En 1996 le CLUSIF arrête ses évaluations (collecte des chiffres trop difficile et résultats trop incertains), pour les reprendre en 2000 et 2001 avec une nouvelle méthode (sondage/interview auprès d'un échantillon de sociétés et correction des résultats selon la représentativité de l'échantillon) et la collaboration d'un cabinet conseil spécialisé [CLUSIF20].

Ces nouvelles études se basent surtout sur la notion binaire de *survenance*, c'est-à-dire la réponse à la question *'avez-vous connu cette année un ou plus d'un sinistre de type X ?'*. Dans la plupart des cas, les personnes interrogées étaient en mesure de répondre à cette question, mais pas de préciser le nombre ni l'impact des sinistres du type spécifié. Des estimations d'occurrence (nombre de sinistres) et d'impact sont cependant données à titre indicatif, mais pour une partie limitée et non représentative de l'échantillonnage total (principalement, les PME).

Cette méthode, qui se veut plus proche de celle utilisée outre-atlantique par le CSI-FBI[45], n'établit malheureusement plus les ventilations en fonction des conséquences primaires (DICW) qui nous avaient intéressées dans les moutures précédentes; de ce fait, ces derniers rapports du CLUSIF ne nous apportent guère d'informations utilisables et ne seront par conséquent pas exploités.

6.4. Identification des menaces significatives

6.4.1. Atteintes à la disponibilité

Pour la période 1991 à 1996, les données du CLUSIF [CLUSIF19] nous indiquent que plus ou moins 85% des conséquences financières des sinistres ayant provoqué un problème de disponibilité[G] ont été causées par des incidents de type A1, A2, E2, M4 et M6 (tableau 6.2.).

Tableau 6.2.	**Ventilation des pertes financières (D) par type de menace[46].** *(principales menaces contribuant au percentile choisi)*[47]							
Type de conséquence	*Rapport*	*Pertes (10^6 FF)*	*Percentile +/- 85*	*Pertes (%) A1*	*Pertes (%) A2*	*Pertes (%) E2*	*Pertes (%) M4*	*Pertes (%) M6*
Disponibilité	1991	4430	85	1000 (23 %)	800 (18 %)	400 (9 %)	400 (9 %)	1150 (26 %)
	1992	4460	85	1020 (23 %)	750 (17 %)	430 (10 %)	420 (9 %)	1150 (26 %)
	1993	4475	87	1090 (24 %)	750 (17 %)	430 (7 %)	440 (10 %)	1170 (26 %)
	1994	4640	84	1130 (24 %)	760 (16 %)	410 (9 %)	440 (9 %)	1170 (25 %)
	1995	4735	85	1170 (25 %)	760 (16 %)	430 (9 %)	445 (9 %)	1230 (26 %)
	1996	5160	84	1450 (28 %)	860 (17 %)	400 (8 %)	270 (5 %)	1350 (26 %)
	1991-1996	27900	85	6860 (25 %)	4680 (17 %)	2500 (9 %)	2415 (9 %)	7220 (26 %)

Les menaces[G] de type M6 ('autres') qui arrivent en tête de ce classement correspondent à un type composé qui requiert une analyse plus fine pour que nous puissions estimer leur pertinence. Les rapports ne sont malheureusement pas très précis à ce sujet, puisqu'ils nous ventilent M6 soit en fonction des conséquences[48]

[44] Le CLUSIF parle dans ce cas de conséquences *financières* ou *indirectes*.
[45] CSI (Computer Security Institute): http://www.gocsi.com
[46] Le tableau complet figure en ANNEXE 3 (tableau A3.1).
[47] Les pourcentages et percentiles ont été arrondis à l'unité, entraînant sur certaines lignes une erreur tout à fait acceptable si on tient compte de la précision annoncée des estimations financières (6.3.2.b).
[48] Les analystes du CLUSIF admettent un certain arbitraire dans la ventilation interne à M6.

(impact sur la disponibilité[G] ou la confidentialité[G]), soit en fonction de la cause (perte de personnel, utilisation abusive de ressources informatiques ou contrefaçon de logiciels) - mais pas des deux.

Pour tenter d'aller plus loin, nous avons imaginé une règle de répartition simple mais plausible (tableau 6.3.):

- nous attribuons en priorité un impact en disponibilité[G] pour la cause *utilisation abusive des ressources informatiques*;
- nous attribuons en priorité un impact en confidentialité[G] pour la cause *contrefaçon de logiciels*;
- le cas échéant, nous complétons l'une ou l'autre valeur d'impact avec les montants attribués à la cause *départ de personnel.*

Tableau 6.3.	**Décomposition de M6 en causes élémentaires (pertes en 10^6 FF)** *Les chiffres en gras sont extraits des rapports; les autres constituent le résultat de notre hypothèse de répartition*				
Rapport	*Critère impacté*	*Total M6 selon critère impacté*	*M6 Facteurs humains*	*M6 Utilisation ressources*	*M6 Copie et contrefaçon*
1991	Disponibilité	**1150**	150 (13 %)	1000 (87 %)	-
	Confidentialité	**1250**	-	-	1250 (100 %)
	Tous critères	**2400**	**150**	**1000**	**1250**
1992	Disponibilité	**1150**	50 (4 %)	1100 (96 %)	-
	Confidentialité	**1280**	80 (6 %)	-	1200 (94 %)
	Tous critères	**2430**	**130**	**1100**	**1200**
1993	Disponibilité	**1170**	40 (4 %)	1130 (97 %)	-
	Confidentialité	**1330**	80 (%)	-	1250 (%)
	Tous critères	**2500**	**120**	**1130**	**1250**
1994	Disponibilité	**1170**	-	1170 (100 %)	-
	Confidentialité	**1530**	100 (7 %)	30 (2 %)	1400 (92 %)
	Tous critères	**2700**	**100**	**1200**	**1400**
1995	Disponibilité	**1230**	-	1230 (100 %)	-
	Confidentialité	**1600**	80 (5 %)	20 (1 %)	1500 (94 %)
	Tous critères	**2830**	**80**	**1250**	**1500**
1996	Disponibilité	**1350**	-	1350 (100 %)	-
	Confidentialité	**1760**	60 (4 %)	-	1700 (97 %)
	Tous critères	**3110**	**60**	**1350**	**1700**
91 - 96	Disponibilité	**7220**	240 (4 %)	6980 (97 %)	-
	Confidentialité	**8750**	400 (5 %)	50 (1 %)	8300 (95 %)
	Tous critères	**15970**	**640**	**7030**	**8300**

Cette clé de répartition indiquerait que sur les 6 années, 97% (en croissance) de la contribution à M6 proviendrait de la cause *utilisation abusive des ressources informatiques*, alors que les trois autres pourcents seraient liées à des *facteurs humains*. Enfin, au niveau de la pertinence de la cause M6, il nous semble pouvoir déclarer que:

- la cause *facteurs humains* peut être ignorée sans que cela mette fondamentalement à mal notre percentile (4% de M6, alors que M6 représente 26% des pertes, cela donne moins de 1% des pertes totales attribuées aux *facteurs humains*);
- *(6.4.1.a)* la cause *utilisation abusive des ressources informatiques* nous paraît pertinente;

Les menaces[G] de types A1 (*accidents physiques*) et A2 (*pannes*) s'avèrent également préoccupantes, mais nous posent un autre problème: si nous devions mettre sur pied les mesures de prévention et de protection adéquates, il nous paraît difficilement contestable que le coût de ces mesures serait supérieur au coût du sinistre éventuel (affectant une application non stratégique et un peu de matériel) [49] *(6.4.1.b)*.

En conclusion, nous dirions qu'en ce qui concerne les atteintes à la disponibilité[G] nous identifions comme causes relevantes principales (par ordre décroissant d'importance):

- M6: utilisation non autorisée des ressources informatiques (estimation: autour de 25% des pertes);

[49] Tenant compte également que les atteintes à la disponibilité[G] du système ne représentaient pas notre plus grande inquiétude (4.8.h), et de notre hypothèse relative à la protection physique de la salle des serveurs (5.2.3.4.b).

- E2: erreurs de conception (estimation: autour de 9% des pertes);
- M4: attaque logique (estimation: autour de 9% des pertes);

6.4.2. Atteintes à la confidentialité

Très intéressants également nous paraissent les chiffres relatifs aux atteintes à la confidentialité[G] (4.8.d), puisque les menaces[G] de type M5 et M6 y représentent les causes de plus de 90% des pertes financières liées aux sinistres ayant eu un impact au niveau de ce critère (tableau 6.4).

Tableau 6.4.	**Ventilation des pertes financières (C) par type de menace[50].** *(principales menaces contribuant au percentile choisi)* [51]				
Type de conséquence	*Rapport*	*Pertes (10^6 FF)*	*Percentile proche de 85*[52]	*Pertes (%) M5*	*Pertes (%) M6*
Confidentialité	1991	2090	93	700 (43 %)	1250 (60 %)
	1992	2190	94	770 (45 %)	1280 (58 %)
	1993	2245	96	820 (47 %)	1330 (59 %)
	1994	2485	96	860 (45 %)	1530 (62 %)
	1995	2605	96	900 (45 %)	1600 (61 %)
	1996	2890	99	1100 (48 %)	1760 (61 %)
	1991-1996	14505	96	5150 (46 %)	8750 (60 %)

A priori surprenante, l'absence de M4 (attaque logique) parmi les menaces[G] dont la perte de confidentialité[G] est une conséquence peut probablement s'expliquer par la classification de ces menaces[G] en M5 (divulgation, qui est le propre d'une perte de confidentialité[G]) *(642a)*.

M6, qui se taille ici la part du lion, nous contraint derechef à un second niveau d'investigation. Si nous nous référons à notre hypothèse précédente (tableau 6.3.), nous pouvons estimer que 95% du montant des pertes en M6 sont la conséquence de la *contrefaçon de logiciel*[53], cause qui ne semble pas devoir s'appliquer à notre cas puisque ni la confidentialité[G] ni l'exploitation (en tant que produit commercial) du logiciel ne sont à considérer. Le reste des pertes assignées à M6 (plus ou moins 5% du total de M6) paraît bien insignifiant tenant compte des valeurs des percentiles du tableau 6.4; nous n'en tiendrons pas compte.

6.4.3. Atteintes à l'intégrité

Les menaces[G] qui portent atteinte à l'intégrité[G] nous interpellent davantage, surtout au niveau de l'étendue possible de leurs conséquences (48a). Et si la probabilité réelle de survenance de ce genre d'atteinte par rapport au code et aux données persistantes (cibles les plus sensibles (4.8.b)) nous a poussé à nuancer l'importance de ce critère (4.8.g), il convient aussi de noter que les analystes du CLUSIF ont inclu l'imputabilité[G] (4.8.e) dans les statistiques relatives à l'intégrité[G], avec comme conséquence définitive que nous devons envisager les chiffres du tableau 6.5 avec la plus grande attention.

Au sommet de la hiérarchie ici, nous identifions clairement les menaces[G] de type M2, suivies par E1, M4 et E2 dans un mouchoir de poche. Force nous est de constater, pourtant, que le profil de notre application ne devrait pas en faire une cible privilégiée pour une forme quelconque de *fraude informatique avec détournement de fonds, de biens ou de services* (M2).

En conclusion, de l'analyse du tableau 6.5 nous déduisons les principaux éléments suivants:

- *(6.4.3.a)* M2 ne semble pas devoir représenter une menace[G] à prendre en considération (le type de l'application ne permettant guère d'en abuser à des fins de détournement de biens et de services);
- *(6.4.3.b)* M4 (attaque logique) est à prendre en considération (usurpation d'identité);

[50] Le tableau complet figure en ANNEXE 3 (tableau A3.2).
[51] Les pourcentages et percentiles ont été arrondis à l'unité, entraînant sur certaines lignes une erreur tout à fait acceptable si on tient compte de la précision annoncée des estimations financières (6.3.2.b).
[52] Nous avons choisi le percentile le plus proche du percentile 85, par défaut ou par excès
[53] Les analystes du CLUSIF admettent un certain arbitraire dans la ventilation interne à M6.

- *(6.4.3.c)* Les erreurs de conception (E2) sont à prendre en considération, surtout dans la mesure où elles peuvent probablement induire des erreurs d'utilisation (E1) par défaut de guidance de l'utilisateur.

Tableau 6.5.	**Ventilation des pertes financières (I) par type de menace[54].** *(principales menaces contribuant au percentile choisi)[55]*						
Type de conséquence	*Rapport*	*Pertes (10^6 FF)*	*Percentile +/- 85*	*Pertes (%) E1*	*Pertes (%) E2*	*Pertes (%) M2*	*Pertes (%) M4*
Intégrité	1991	3840	85	580 (15 %)	500 (13 %)	1700 (44 %)	500 (13 %)
	1992	3790	85	640 (17 %)	510 (13 %)	1500 (40 %)	580 (15 %)
	1993	4090	83	640 (16 %)	520 (13 %)	1630 (40 %)	620 (15 %)
	1994	4075	87	700 (17 %)	520 (13 %)	1620 (40 %)	695 (17 %)
	1995	4220	85	700 (17 %)	550 (13 %)	1670 (40 %)	730 (17 %)
	1996	4670	86	700 (15 %)	600 (13 %)	2100 (45 %)	820 (18 %)
	1991-1996	24685	86	3960 (16 %)	3200 (13 %)	10220 (41 %)	3945 (16 %)

6.4.4. Synthèse

Dans les paragraphes précédents, nous avons identifié pour chaque critère les types de menaces[G] responsables d'environ 85% du montant total estimé des pertes financières consécutives aux sinistres correspondants; ensuite, nous avons éliminé certaines menaces[G] non relevantes ou contre lesquelles les éventuelles mesures de prévention ou de protection s'avéreraient économiquement injustifiées. Les résultats obtenus n'en demeurent pas moins relativement bruts puisque les critères eux-mêmes sont considérés comme équivalents entre eux. Or, deux éléments les distinguent fondamentalement les uns des autres:

- l'importance relative que nous leur avons attribuée aux chapitres précédents et
- la part de chacun d'entre eux dans le total de la sinistralité informatique recensée.

La *part relative de chaque critère dans le total de la sinistralité informatique recensée*, renseignée sur le tableau 6.6, nous fournit une indication supplémentaire quant aux parts relatives de chaque type de menace[G] estimée pertinente par critère et provenant des tableaux 6.2, 6.4 et 6.5. Par exemple, la contribution de E2 dans les pertes financières liées à un problème de disponibilité[G] étant en moyenne de 9 % sur les 6 années considérées (tableau 6.2), sa contribution dans les pertes financières totales pour la même période sera estimée à 9 % de 42 % soit 4 %.

Tableau 6.6.		**Ventilation des pertes financières par critère[56].**		
Rapport	*Pertes (10^6 FF)*	*Disponibilité*	*Confidentialité*	*Intégrité Imputabilité*
1991	10360	4430 (43 %)	2090 (20 %)	3840 (47 %)
1992	10440	4460 (43 %)	2190 (21 %)	3790 (46 %)
1993	10810	4475 (41 %)	2245 (21 %)	4090 (48 %)
1994	11200	4640 (41 %)	2485 (22 %)	4075 (46 %)
1995	11560	4735 (41 %)	2605 (23 %)	4220 (47 %)
1996	12720	5160 (41 %)	2890 (23 %)	4670 (47 %)
Totaux	**67090**	**27900 (42 %)**	**14505 (22 %)**	**24685 (47 %)**

Le tableau récapitulatif ci-dessous (tableau 6.7) ordonne les critères de manière conforme à l'expression de nos besoins de sécurité et, pour chaque menace[G] préalablement sélectionnée, fournit une indication de la contribution totale de cette menace[G] par rapport à l'ensemble des pertes financières estimées selon la méthode de calcul illustrée ci-dessus. Ce tableau nous indique que 44 % (le total du tableau) des pertes financières estimées liées à des sinistres informatiques recensés pour la période 1991 - 1996 sont consécutives à des menaces[G] que nous avons estimées relevantes par rapport à notre application.

[54] Le tableau complet figure en ANNEXE 3 (tableau A3.3).

[55] Les pourcentages et percentiles ont été arrondis à l'unité, entraînant sur certaines lignes une erreur tout à fait acceptable si on tient compte de la précision annoncée des estimations financières (6.3.2.b).

[56] Les pourcentages ont été arrondis à l'unité, entraînant sur certaines lignes une erreur de 1% tout à fait insignifiante si on tient compte de la précision annoncée des estimations financières (6.3.2.b).

Ce tableau nous indique également que, abstraction faite de notre critère d'écologie[G], non représenté, des mesures adéquates prises par rapport aux types de menaces[G] E1, E2, M4 et M5 (responsables de 33 % des pertes totales) devraient satisfaire amplement nos besoins de sécurité tels qu'établis au chapitre 4, le solde (M6, 11% des pertes totales) affectant un critère de surcroît déjà considéré comme étant le moins critique (4.8.h).

Tableau 6.7.	**Tableau récapitulatif**[57] *(classement et pondération des types de menaces)*					
Besoin de sécurité (ordre décroissant) selon (4.8).	*Type de conséquence*	*E1*	*E2*	*M4*	*M5*	*M6 (utilisation non autorisée des ressources)*
Ecologie (utilisation de la bande passante)	n/a					
Confidentialité	Confidentialité				8 %	
Imputabilité puis Intégrité	Intégrité	6 %	5 %	6 %		
Ecologie (adaptations de configuration)	n/a					
Disponibilité	Disponibilité		4 %	4 %		11 %

6.4.5. Mesures proposées

Les mesures que nous pourrions envisager pour parer ces menaces[G] relativement génériques dépendent de ce que pourrait être leur mode d'expression. Nous avons vu, par exemple, que dans notre cas M6 s'exprimera préférentiellement par le biais de l'utilisation non autorisée de ressources informatiques. Le tableau 6.8 reprend, en regard de chaque menace[G], son ou ses mode(s) d'expression le(s) plus probable(s) et le ou les type(s) de mesure(s) qui nous semblent le(s) plus approprié(s).

Tableau 6.8.		**Tableau récapitulatif**[58] *(classement et pondération des types de menaces)*
Menaces	*Modes d'expression privilégié*	*Types de mesures*
E1	DoS involontaire (à l'encontre de soi-même ou d'un autre utilisateur)	*(6.4.5.a)* Formation des utilisateurs *(6.4.5.b)* Documentation utilisateurs
E2	Défaut d'ergonomie (guidance des utilisateurs) entraînant des vulnérabilités par rapport à la menace E1	*(6.4.5.c)* Conception ergonomique simple, dépouillée et intuitive
	Erreurs diverses de conception ou de développement entraînant des vulnérabilités par rapport à l'imputabilité (M4), la disponibilité ou l'écologie.	*(6.4.5.d)* Soin particulier à apporter à la sélection des méthodes de conception et de développement ainsi qu'au cycle de vie du produit.
M4	Usurpation d'identité et attaques de type DoS	*(6.4.5.e)* Mesures techniques : choix et/ou implémentation des (types de) protocoles (authentification, communication, autres)
M5	Divulgation de ses codes d'accès par un utilisateur	*(6.4.5.f)* Formation des utilisateurs (sensibilisation à la sécurité) *(6.4.5.g)* Utilisation conjointe d'une authentification biométrique.
	Autres divulgations (identité des clients, nature de leurs problèmes, etc.)	*(6.4.5.h)* Formation des utilisateurs (sensibilisation à la sécurité)
M6	Utilisation abusive des ressources du système (communication entre clients, utilisation du système par des personnes non autorisées)	*(6.4.5.i)* Nécessité et confidentialité de l'authentification. *(6.4.5.j)* Confidentialité de l'enrôlement. *(6.4.5.k)* Confidentialité des données persistantes.

[57] Les pourcentages ont été arrondis à l'unité, entraînant sur certaines lignes une erreur de 1% tout à fait insignifiante si on tient compte de la précision annoncée des estimations financières (6.3.2.b).

[58] Les pourcentages ont été arrondis à l'unité, entraînant sur certaines lignes une erreur de 1% tout à fait insignifiante si on tient compte de la précision annoncée des estimations financières (6.3.2.b).

6.5. Evaluation de l'approche

Si dans l'absolu la validité d'une approche statistique nous paraît claire, il nous faut toutefois concéder qu'en pratique cette dernière nous pose de nombreux problèmes dont les principaux sont de l'ordre de la démarche elle-même mais aussi de la disponibilité, de la représentativité et de la fiabilité des données.

Du point de vue de *la démarche*, nous ne sommes pas convaincus que l'expression statistique de la sinistralité en termes de pertes financières représente une bonne base de comparaison et d'analyse. Comment, en effet, pouvons-nous transposer d'un contexte à l'autre des estimations financières parfois très approximatives ? On imagine aussi aisément la nature de l'impact qu'aurait sur ces données, par exemple, un seul sinistre affectant un secteur particulièrement sensible d'une très grosse entreprise; la quantification de la sinistralité sur base du critère financier est probablement moins intéressante ici que ne l'aurait été la seule mesure du taux d'incidence (parfois appelé occurrence) d'un type de sinistre. Enfin, parmi les autres inconvénients relatifs à la démarche, citons encore l'absence de possibilité de représentation d'autres critères plus spécifiques (comme notre critère d'écologie[G]), l'absence de recommandations de nature à contrer les causes relevantes identifiées et la difficulté de classification pour certains types de causes (M6 par exemple).

Au chapitre de la *disponibilité des données*, nous devons avouer que nous ne sommes pas parvenu à trouver d'autres données exploitables que celles du CLUSIF. Aucun des autres clubs 'frères' (CLUSIT en Italie, CLUSIB en Belgique, CLUSIS en Suisse, ...) ne dispose de ce genre de statistiques; d'autres organismes n'ont jamais répondu aux questions que nous leur avons posées à ce sujet (ASIRQ, ...) et quand il est arrivé que nous trouvions finalement d'autres données, comme par exemple auprès du CSI, ces données paraissaient suspectes ou inexploitables dans notre contexte pour une ou plusieurs des raisons suivantes:

- le métier de l'organisme: tel qui vend de la sécurité logique met en exergue les problèmes des pirates informatiques, des virus et de la connexion à l'Internet, passant parfois totalement sous silence les accidents et les erreurs;
- le mode de présentation des données ne permet pas leur ventilation par type de cause et type de conséquence;
- parfois, ces données sont tout simplement confidentielles.

Une piste que nous n'avons toutefois pas exploitée, et où des informations existent plus que certainement, est celle des compagnies d'assurances. Là aussi, cependant, nous craignons que les informations relatives aux sinistres recensés soient considérées comme confidentielles.

La *représentativité des données* nous amène également un certain nombre de commentaires:

- il semble douteux que nous puissions encore réellement tirer des enseignements valables à partir de données statistiques qui, comme celles exploitées ici, datent des années 1991 à 1996;
- notre entreprise, notre contexte, notre application représentent autant de spécificités qui nous éloignent probablement du profil des entreprises[59] et types d'applications qui ont permis l'élaboration des données utilisées (6.3.2.a.).

Enfin, pour ce qui est de la *fiabilité des données*, nous rappellerons simplement que la marge d'erreur sur les estimations des pertes financières est estimée à près de 30% (6.3.2.b); la difficulté d'estimation de ces pertes financières a par ailleurs conduit le CLUSIF à changer sa méthode d'investigation.

En conclusion, il nous semble qu'une approche basée sur des données statistiques est intéressante en soi mais souffre grandement du manque de données fiables et exploitables et ne peut donc, dans le meilleur des cas, que venir en complément ou illustration d'une autre démarche.

[59] Pour l'établissement de ses rapports 2000 et 2001, le CLUSIF a introduit un mode de correction des données qui tient compte de la représentativité de l'échantillonnage.

Chapitre 7 La méthode du CEA

Le point de vue du *Comité Européen des Assurances* (CEA) sur l'identification des menaces[G].

7.1. Introduction

7.1.1. Pourquoi le CEA

Nous avons choisi de consacrer un peu de temps à la méthode du CEA pour les raisons suivantes:

- c'est le CEA qui a établi la *grille harmonisée des menaces*[G] *informatiques* que nous avons utilisée au chapitre précédent;
- la méthode du CEA propose des recommandations concrètes pour améliorer la sécurité;
- la méthode du CEA est atypique parce que destinée en première approche à des non informaticiens, et à ce titre susceptible de nous apporter un éclairage inhabituel.

Toutefois nous tenons à préciser d'emblée que le développement de cet outil semble avoir été abandonné avant qu'il soit arrivé à maturité.

7.1.2. Contexte historique

Créé en 1953, le Comité Européen des Assurances ou CEA[60] est la fédération des Associations nationales des compagnies d'assurances européennes. Son objectif principal consiste à promouvoir, défendre et illustrer les positions de ses membres dans les débats économiques et sociaux ayant cours à une échelle supranationale.

Devant l'émergence d'une nouvelle catégorie de sinistres liés à l'emploi des technologies de l'information, le CEA a créé en 1991 une commission *Assurance et Sécurité des Risques*[G] *Informatiques*, avec pour mission d'étudier les caractéristiques propres des sinistres informatiques, d'en évaluer les conséquences potentielles et, devant une sinistralité parfois sérielle et transfrontalière, de proposer à tous ses membres des outils communs d'évaluation du risque[G] informatique.

7.1.3. Audience

L'outil développé par la commission précitée était destiné à permettre aux assureurs eux-mêmes de conduire, rapidement et facilement, un premier audit de sécurité. Ce n'est que si la complexité ou l'interconnexion des systèmes le justifiait que le concours d'un professionnel des TI s'avérait indispensable.

7.1.4. Matériel

Le CEA a gracieusement mis à notre disposition ce qui pourrait bien constituer l'unique publication décrivant leur méthode, alors encore au stade de développement [CEA].

7.1.5. Principe

Le principe de la méthode CEA est extrêmement simple à énoncer et consiste en 4 phases:

- *(7.1.5.a)* sur base d'un questionnaire destiné à l'évaluation d'un *système existant*, l'assureur est supposé pouvoir mettre en évidence les éventuelles vulnérabilités[G] (phase 1).
- *(7.1.5.b)* Cette tâche accomplie, il procède avec son client à la définition du *seuil du tolérable*[61] (phase 2),
- *(7.1.5.c)* seuil sur base duquel les menaces[G] significatives sont identifiées (phase 3).

[60] http://www.cea.assur.org

[61] Ce que nous pourrions comparer à une expression quantifiée des besoins en sécurité.

- *(7.1.5.d)* Il ne reste plus alors qu'à traiter ces menaces[G] en proposant (voire en imposant) une série de recommandations (phase 4). Bien entendu, ces recommandations ne sont pas à prendre au sens strict mais doivent toujours faire l'objet d'une évaluation et d'une adaptation au contexte particulier.

Conceptuellement, les phases résumées ci-dessus correspondent plus ou moins à une approche traditionnelle telle que celle utilisée dans ce document:

- l'expression des besoins de sécurité (notre deuxième partie) peut s'apparenter à la première phase (7.1.5.a) de la méthode du CEA; toutes deux produisent des résultats plus ou moins comparables, à savoir une liste des besoins de sécurité pour l'une, et une liste des vulnérabilités[G] pour l'autre;
- l'identification des menaces[G] (notre troisième partie) correspond aux phases 2 (7.1.5.b) et 3 (7.1.5.c) du CEA: en sortie, les deux approches produisent une liste de menaces[G] significatives à prendre en considération;
- la définition des exigences (notre cinquième partie) pourrait emprunter une partie de son contenu à la phase 4 (7.1.5.d) de la méthode du CEA (détermination des recommandations de sécurité).

Toutefois la méthode du CEA, destinée à l'évaluation d'un existant en vue de l'établissement d'une couverture d'assurance, n'a pas l'ampleur de la plupart des méthodes issues du monde des TI, et c'est la raison pour laquelle elle sera entièrement visitée dans ce seul chapitre.

La méthode du CEA s'articule aussi autour de quatre outils:

- *(7.1.5.e)* une *grille harmonisée des menaces*[G] *informatiques* destinée à la collecte et au traitement d'informations statistiques concernant la sinistralité (comme par exemple l'utilisation qu'en a faite le CLUSIF au chapitre précédent) mais aussi à la description des garanties offertes;
- *(7.1.5.f)* un questionnaire d'audit permettant aux assureurs et utilisateurs de mettre rapidement en évidence les éventuels défauts en matière de sécurité;
- *(7.1.5.g)* une série de tables de références croisées (questions par rapport aux types de menaces[G], fiches de recommandations par rapport aux types de menaces[G]);
- *(7.1.5.h)* une collection de fiches de recommandations destinée, en conjonction avec le questionnaire d'audit, à proposer des pistes ou des solutions d'amélioration de la sécurité.

7.2. Présentation des outils

7.2.1. La grille harmonisée des menaces informatiques

La *grille harmonisée des menaces*[G] *informatiques* (7.1.5.e), que nous avons introduite en (6.2.2), identifie treize types de menaces[G] répartis en trois catégories: les accidents ('A'), les erreurs ('E') et les actes de malveillance ('M'). En regard de chaque type de menace[G] figurent 6 colonnes correspondant aux six types de conséquences financières (numérotées 'C1' à 'C6') répartis en deux catégories: les *conséquences financières directes* et les *conséquences financières indirectes*. Le lecteur trouvera en ANNEXE 4 les définitions exactes des types de menaces[G] et de conséquences de la grille représentée par la tableau 7.1. Pour résumer, nous dirons simplement ici que:

- les *conséquences financières directes* reprennent tous les frais d'expertise, de remplacement, de restauration des éléments matériels (C1) ou logiciels (C2) détruits ou endommagés;
- les *conséquences financières indirectes* reprennent les frais nécessaires à maintenir (autant que faire se peut) le système opérationnel jusqu'à réparation / restauration complète et les pertes d'exploitation (C3), les pertes de fonds et de biens (C4), la responsabilité civile éventuelle (C5) et tous les autres types de pertes (C6) comme la détérioration de l'image de marque, etc.

7.2.2. Le questionnaire d'audit et les fiches de recommandations

Le CEA projetait l'établissement d'un questionnaire d'audit (7.1.5.f) à trois niveaux, chaque niveau supérieur au premier venant en complément du niveau précédent. Dans leur optique, l'assureur devait toujours pratiquer lui-même l'audit de premier niveau et si possible aussi celui du deuxième niveau. Le questionnaire de premier niveau était destiné à mettre en évidence rapidement les principales anomalies de sécurité, l'audit de second voire de troisième niveau étant alors prévu selon la complexité du système où l'importance de la couverture.

Tableau 7.1	**Grille harmonisée des menaces informatiques**					
Types de conséquences:	*Conséquences financières directes*		*Conséquences financières indirectes*			
Types de menaces	*C1*	*C2*	*C3*	*C4*	*C5*	*C6*
Catégorie 'A' - Accidents						
A1 Physiques						
A2 Pannes						
A3 Evénements naturels						
A4 Perte de services						
A5 Autres						
Catégorie 'E' - Erreurs						
E1 Erreurs d'utilisation						
E2 Erreurs de conception						
Catégorie 'M' - Malveillance						
M1 Vol						
M2 Fraude						
M3 Sabotage						
M4 Attaque logique						
M5 Divulgation						

En regard de chaque question sont renseignés le ou les type(s) de menaces[G] couverts ainsi qu'une appréciation de l'importance de la question en termes de contrôle des sinistres visés[62]. A noter que seuls les questionnaires de premier et de second niveau ont été établis.

Tableau 7.2	**Exemple de question (question 12)**		
Niveau 1	*Niveau 2*	*Risques couverts*	*Importance*
12: Existe-t-il une installation d'extinction d'incendie adaptée (au moins extincteurs portatifs et si possible installation d'extinction automatique à eau ou à gaz, tenant compte de la disposition des locaux et des caractéristiques des contenus, faisant l'objet de procédures contrôlées et de tests périodiques d'efficacité ?	**12/1:** Y a-t-il une installation exhaustive de détection précoce d'incendie avec report à une centrale d'alarme ? **12/2:** Dispose-t-on du nombre et de la répartition réglementaire d'extincteurs manuels à contenu adapté au type de feu attendu ? **12/3:** La climatisation est-elle automatiquement coupée en cas d'alarme incendie ?	A1 M3	* * *

A chacune des 28 questions établies au niveau 1 et couvrant les aspects organisationnels, de sécurité physique et de sécurité logique correspond une fiche de recommandations (7.1.5.h); ces fiches comportent de un à trois niveaux de recommandations[63] présentées de manière synthétique, mais souvent suivies d'une explication plus détaillée. Le lecteur trouvera en ANNEXE 5 plusieurs exemples de fiches de recommandations.

Pour terminer, une table croisée des menaces[G] par les questions (7.1.5.g) permet l'accès direct aux questions qui relèvent d'un problème particulier.

7.3. Identification des menaces significatives

7.3.1. Avertissement

La démarche que nous allons suivre n'est pas celle de l'audit traditionnel d'un système existant tel que présenté en (7.1.5), mais plutôt d'un audit ciblé autour d'un certain nombre de préoccupations relevantes. Clairement, ce qui nous intéresse ici n'est pas l'audit (phase 1) mais l'identification des menaces[G].

[62] Evaluation simple à 3 niveaux: (*) = moyennement important, (**) = important, (***) = très important.
[63] Les recommandations minimales (ou R1), renforcées (ou R2) et très renforcées (ou R3).

7.3.2. Identification des vulnérabilités

L'identification des vulnérabilités[G] est normalement réalisée par l'utilisation des questionnaires d'audit (7.1.5.f) par rapport à un système existant. Notre approche étant différente ici (le système restant à définir), nous nous baserons sur les résultats de l'expression de nos besoins en matière de sécurité (la deuxième partie de ce document), considérant toute atteinte à ces objectifs comme signe d'une vulnérabilité[G] potentielle.

Ces vulnérabilités[G] s'expriment donc en termes de conséquences *fonctionnelles*[64] plutôt qu'en termes de conséquences *financières* (C1 à C6). Il serait probablement possible d'évaluer des conséquences financières, mais nous avons préféré nous en abstenir pour les raisons suivantes:

- estimer l'impact financier d'un sinistre qui n'a pas eu lieu serait plus imprécis encore que l'estimation des conséquences financières de sinistres ayant eu lieu. Hors, l'incertitude sur ces estimations a déjà été mise en évidence par le CLUSIF (6.3.2.b);
- nous ne disposons d'aucun élément nous permettant de déterminer le *seuil du tolérable* en termes de pertes financières pour l'entreprise.

7.3.3. Définition du seuil du tolérable

Le problème de la définition du *seuil du tolérable* (7.1.5.b) peut être approché par l'utilisation d'un niveau de gravité *G* définit par [CEA] comme suit:

- le niveau de gravité *G* vaut '1' en cas de conséquences faibles ou acceptables (un sinistre ne bouleverserait pas les objectifs stratégiques de l'entreprise);
- le niveau de gravité *G* vaut '2' en cas de conséquences graves ou très graves (un sinistre bouleverserait les objectifs stratégiques de l'entreprise);
- le niveau de gravité *G* vaut '3' en cas de conséquences catastrophiques mettant en danger la pérennité de l'entreprise;
- le seuil du tolérable se situe entre '1' et '2'.

Cette définition du niveau de gravité ayant déjà inspiré nos critères d'évaluation définis en 4.2 et utilisés tout au long du chapitre 4, nous reprendrons comme vulnérabilités[G] significatives ci-dessous les atteintes ayant fait monter au moins jusque '2' la cote de notre évaluation globale (4.8).

Tableau 7.3	**Vulnérabilités significatives** *(seuil du tolérable atteint ou dépassé)*			
#	*Définition / description*	*G='1'*	*G='2'*	*G='3'*
1	Problème d'écologie par rapport à la bande passante (4.8.c)		(4.6.5.f) (4.6.5.g)	
2	Problème de confidentialité (4.8.d)		(4.4.2.e)	
3	Problème d'imputabilité (4.8.e)		(4.5.2.a) (4.5.2.b) (4.5.2.d)	
4	Problème d'intégrité (4.8.f)		(4.7.2)	
5	Problème d'écologie par rapport aux configurations de sécurité (4.8.g)			(4.6.5.b)

7.3.4. Identification des menaces

L'identification des menaces[G] (7.1.5.c) qui s'effectue en parcourant la *grille harmonisée des menaces*[G] (7.1.5.e) *informatiques* (tableau 7.1) consiste, pour chacun des 13 types, à se poser les questions suivantes:

- ce type de menaces[G] est-il de nature à exploiter une des vulnérabilités[G] significatives identifiées au tableau 7.3 ?
- si oui, et en cas de sinistre majeur, quel pourrait en être l'impact ?

[64] C'est-à-dire les types de conséquences appelées *primaires* ou *directes* (disponibilité[G], intégrité[G], imputabilité[G]) dans les rapports du CLUSIF.

Nous reportons ensuite au tableau 7.4 l'estimation de l'impact d'un sinistre majeur pour chaque type de menaces[G] dans la colonne correspondant à la vulnérabilité[G] en question.

Pour bien évaluer les critères liés à l'écologie[G], il convient de garder en tête que nous considérons en entrée les types de menaces[G] *affectant notre application* et non ceux qui en sont une résultante. Par exemple, une erreur de conception de notre application peut générer une consommation accrue de bande passante, laquelle induit *pour les autres applications* une perte de services essentiels, d'où un impact d'un niveau 2. Selon ce même raisonnement, c'est bien une erreur de conception de notre application qui nous obligerait à modifier nos configurations de sécurité, lesquelles modifications - qu'elles soient démesurées dans leurs spécifications ou mal implémentées - représentent une menace[G] majeure (niveau 3).

Tableau 7.4	**Identification des menaces.**						
Types de menaces	*Libellé*	*Gravité par vulnérabilité (identifiées au tableau 7.3)*					
		1	*2*	*3*	*4*	*5*	*Max.*
A1	Accident physique						
A2	Pannes						
A3	Force majeure						
A4	Perte de services						
A5	Autres accidents						
E1	Erreurs d'utilisation		2	2			2
E2	Erreurs de conception	2	2	2	2	3	3
M1	Vol		2	2	2		2
M2	Fraude						
M3	Sabotage						
M4	Attaque logique	2	2	2	2		2
M5	Divulgation		2	2	2		2
M6	Autres (départ de personnel)		2	2	2		2

Ce qui nous donne la classification suivante:

- type de menaces[G] de premier rang:
  - *(7.3.4.a)* E2 (erreurs de conception ou de réalisation[65]) est identifié comme type de menaces[G] principal, avec impact possible par rapport à chacun de nos critères;
- type de menaces[G] de deuxième rang:
  - *(7.3.4.b)* M4 (attaque logique) arrive en second lieu, avec impact possible sur 4 des 5 critères; tenir compte que M4 ouvre traditionnellement la porte à M5 (par rapport à l'intégrité[G] et l'imputabilité[G])
- types de menaces[G] de troisième rang:
  - *(7.3.4.c)* M5 (divulgation), possiblement en résultante d'une menace[G] de type M4. Ce type de menaces[G] ne pourra être efficacement contré que par des mesures organisationnelles qui sortent du cadre de ce document.
  - *(7.3.4.d)* M6 (départ de personnel). Ce type de menaces[G] ne pourra être efficacement contré que par des mesures organisationnelles qui sortent du cadre de ce document.
  - *(7.3.4.e)* M1 (vol de matériel) est perçu comme un type de menaces[G] par rapport aux critères de confidentialité[G], d'intégrité[G] et d'imputabilité[G];
- et en dernier rang:
  - *(7.3.4.f)* E1 (erreurs d'utilisation) aurait un impact en confidentialité[G] et en imputabilité[G].

Si nous comparons ces résultats à ceux que nous avait procuré l'approche statistique, nous retrouvons en général les mêmes types de menaces[G] (E1, E2, M4 et M5) ce qui n'est pas vraiment surprenant puisque:

- les deux approches ont été réalisées par la même personne;
- les deux approches sont fondées sur les mêmes données de base établies dans le chapitre 4, données par conséquent constituées uniquement de vulnérabilités[G] (ou besoins de sécurité) déjà élevé(e)s;

[65] Concerne aussi bien un développement qu'une adaptation de configuration.

- les deux approches utilisent la même classification des types de menaces[G], qui n'en compte quand même que 13;

Trois différences majeures méritent toutefois d'être à signalées:

- en ce qui concerne M6: d'après l'approche statistique, la plus grande menace[G] provenait de l'*utilisation non autorisée des ressources*, alors que d'après la réflexion basée sur la méthode du CEA (tableau 7.4) c'est le *départ de personnel* qui nous a semblé plus préoccupant. Mais il s'agit là d'une appréciation totalement subjective;
- enfin, l'apparition ici du type de menaces[G] M1 (vol). Dans les rapports statistiques, M1 apparaissait mais de manière marginale (quoique en augmentation); nous interprétons sa présence ici par le fait que la méthode du CEA ne permet pas de quantification (prise en considération de l'occurrence réelle) des types de menaces[G], alors que quand nous parlons de statistiques, une part de quantification implicite existe toujours;
- enfin notons encore l'absence d'impact de E1 en disponibilité, qui est à imputer au fait que les atteintes à la disponibilité n'ont pas été retenues lors de la définition de notre seuil du tolérable (tableau 7.3).

7.4. Traitement des menaces

7.4.1. Sélection des fiches de recommandations

A partir d'ici le traitement des types menaces[G] consiste à sélectionner et appliquer les recommandations de la méthode. Sur base de la grille croisée des fiches de recommandation par type de menaces[G] (7.1.5.g) ([CEA] page 47)[66], nous organisons les recommandations en procédant comme suit:

- les fiches de recommandations importantes (marquées de 3 étoiles) sont à considérer en priorité;
- le niveau de la recommandation à considérer doit être le niveau le plus élevé disponible qui ne soit pas supérieur au niveau de gravité maximum indiqué au tableau 7.4 en regard du type de menaces[G] considéré.

Si nous prenons successivement en compte les types de menaces[G] E2, M4, M5, M1 et E1 en entrée dans le tableau de la page 47 [CEA] [67], nous sélectionnons (respectivement aux niveaux R3 et R2 quand ils existent) 23 fiches de recommandations (sur un total de 28), dont 2 prioritaires (***), 11 secondaires (**) et 12 facultatives (*) (tableau 7.5 page suivante).

7.4.2. Evaluation des recommandations

Le travail de sélection ne s'arrête pas pour autant puisque chaque fiche doit maintenant être étudiée, son adéquation par rapport au contexte validée (sinon la fiche peut être écartée) et la recommandation éventuellement adaptée aux spécificités. Par rapport à notre contexte particulier, les fiches de recommandations sélectionnées nous inspirent les commentaires suivants:

- Le vol (M1), dont le poids global dans la sinistralité reste faible mais croît avec la décentralisation [CLUSIF19], concerne principalement du matériel nomade (laptops) ou du petit matériel (consommables: cartouches d'imprimantes, etc.). Dans notre projet d'application, ce type de menaces[G] ne devrait pas porter à conséquence si nous respectons les deux règles suivantes:
  - *(7.4.2.a)* que le serveur lui-même soit un minimum protégé (fiche 9);
  - *(7.4.2.b)* qu'aucune information (code d'accès, répertoire, ...) ne soit enregistrée sur les postes clients (4.4.3.e).

[66] De nombreuses contradictions émaillent le document [CEA]; par exemple la grille de la page 47 renseigne la fiche 27 comme relevante par rapports aux types de sinistres E2 et M1 à M5 alors que la même fiche annonce un champ d'application qui serait A1, A4, E1, E2, M1, M2 et M3. Des contradictions similaires existent aussi avec les tableaux des pages 34 et 35 du même document, ainsi qu'avec le questionnaire d'audit qui précède. Nous n'avons pas voulu assumer ici un rôle de correcteur, et avons donc choisi de nous baser exclusivement sur le tableau de la page 47.

[67] Faisant l'impasse sur M6 qui ne figure pas dans ce tableau.

Des fiches assignées à 'M1' (tableau 7.5), nous ne retiendrons donc que la fiche numéro 9[68].

Tableau 7.5	**Sélection des fiches de recommandations.**			
1. - Mesures prioritaires (***)				
Type de Menace [69]	*Fiche*	*Importance*	*Niveau*	*Objet de la recommandation*
M4	19	***	R2	Sauvegardes: plans, rotation, transfert, restauration.
M4	20	***	R2	Authentification et contrôle d'accès logique; audit.
2. - Mesures secondaires (**)				
Type de Menace	*Fiche*	*Importance*	*Niveau*	*Objet de la recommandation*
E2	2	**	R2	Structure sécurité: ressources accordées au responsable de la sécurité
E2	5	**	R2	Analyse des risques: utilisation d'une méthode formelle reconnue
E2	6	**	R1	Procédures de sécurité: formalisation écrite
E2	7	**	R3	Audit: faire procéder à des tests d'intrusion
M1	9	**	R2	Bâtiments: compartimentage selon fonction des locaux, et contrôles d'accès.
M1	13	**	-	- [70]
M4	16	**	R2	Contrôle des accès physiques: enregistrement des visiteurs, (télé)surveillance
E2	22	**	R3	Sécurité IT: méthodologie rigoureuse (développement, réception, administration, contrôles) et chiffrement des données
E2	27	**	R2	Journalisation de la maintenance: évolutions et incidents (patches, versions, ...)
3. - Mesures facultatives (*)				
Type de Menace	*Fiche*	*Importance*	*Niveau*	*Objet de la recommandation*
E2	1	*	R3	Education: sensibilisation régulière de l'ensemble du personnel
E2	3	*	R1	Environnement social: renforcement des mesures si l'environnement social / humain présente un risque
E2	4	*	R3	Classification des objets: étiquetage rigoureux (propriétaire, valeur DIC, ...)
M1	8	*	R2	Environnement: mesures de prévention, de protection et de détection.
M1	10	*	R2	Bâtiments informatiques: appropriation des locaux pour salles informatiques.
M1	11	*	R2	Sécurité infrastructure: compartimentage
M1	15	*	-	- [71]
M4	21	*	R2	Journalisation: enregistrement et analyse de l'audit d'exploitation (activité)
E2	23	*	R2	Documentation: sauvegarde et protection
M4	25	*	R1	Médiathèque: contrôle des accès et procédures de gestion
M4	26	*	R1	Accès aux salles informatiques: limité au personnel nécessaire
E2	28	*	R2	Sécurité de l'exploitation: suivi et contrôle d'exploitation

- Au niveau des recommandations prioritaires (fiches résiduelles):
  - la fiche 19 (plans, rotation, transfert des sauvegardes) n'est pas très pertinente dans la mesure où les seules données persistantes seraient des données statiques (profils utilisateurs);
  - *(7.4.2.c)* la fiche 20 est pertinente (granularité d'accès, mots de passe modifiables);
- Au niveau des recommandations secondaires (fiches résiduelles):

[68] La plupart des autres fiches assignées à M1 semblent, curieusement, surtout concerner des accidents physiques ou un sabotage (M3) qui pourrait en être la cause.

[69] Lorsqu'une fiche est sélectionnée par plusieurs types de menaces[G], nous l'assignons au type dominant qui sera celui auquel correspondra le niveau de gravité *G* le plus élevé (tableau 7.4), puisque c'est *G* qui détermine le niveau de la recommandation à utiliser si disponible. En cas d'égalité de niveau de gravité, nous l'assignons au type de menaces[G] qui aurait un impact par rapport à un plus grand nombre de vulnérabilités (tableau 7.4).

[70] La seule recommandation de cette fiche est une recommandation de niveau 3 (R3).

[71] La seule recommandation de cette fiche est une recommandation de niveau 3 (R3).

- la fiche 2 (attribution de ressources humaines et financières en suffisance au responsable de la sécurité) est inapplicable faute de budget et de personnel (1.2.3.b);
- *(7.4.2.d)* la fiche 5 (utilisation d'une méthode formelle reconnue) est pertinente;
- *(7.4.2.e)* la fiche 6 (formalisation écrite des procédures de sécurité) est pertinente;
- *(7.4.2.f)* la fiche 7 (tests d'intrusion) est pertinente mais l'efficacité de cette recommandation pâtira du fait que faute de budget (1.2.3.b), c'est la même équipe (voire la même personne) qui s'occupera du développement du projet, de sa sécurité et des tests d'intrusion;
- la fiche 16 (contrôle et enregistrement des visiteurs, cartes d'accès, télésurveillance) est inapplicable faute de budget et de personnel (1.2.3.b);
- *(7.4.2.g)* la fiche 22 (chiffrement des données, méthodologie de développement, de réception, de test) est pertinente;
- *(7.4.2.h)* la fiche 27 (journalisation de la maintenance) est pertinente;

- Enfin, en ce qui concerne les recommandations facultatives (fiches résiduelles):
  - *(7.4.2.i)* la fiche 1 (sensibilisation du personnel) est pertinente et devrait s'étendre à l'ensemble des utilisateurs du système;
  - la fiche 3 (menace[G] au niveau de l'environnement social ou humain) n'est pas d'application;
  - *(7.4.2.j)* la fiche 4 (étiquetage DIC et définition d'un propriétaire par objet) est pertinente, mais son application telle quelle au contexte particulier de l'entreprise et du projet (1.2.3.a) (1.2.3.b) ne paraît pas réaliste. En mode dégradé (R1), cette fiche nous recommande de recenser les objets (ce qui fut fait pour notre nouvelle application au chapitre 5, tableaux 5.2 et 5.4) et de leur attribuer à chacun un responsable fonctionnel (ou administrateur);
  - *(7.4.2.k)* la fiche 21 (enregistrement et analyse de l'audit d'exploitation) est pertinente, sachant toutefois que pour raisons de confidentialité[G] (4.5.1.a) cet audit sera limité par exemple aux seuls échecs d'authentification[G];
  - *(7.4.2.l)* la fiche 23 (établissement et sauvegarde de la documentation) est pertinente;
  - la fiche 25 (accès à la médiathèque) n'est pas davantage pertinente que la fiche 19 (voir ci-dessus);
  - *(7.4.2.m)* la fiche 26 (restriction d'accès aux salles informatiques) est pertinente.
  - *(7.4.2.n)* la fiche 28 (suivi et contrôle d'exploitation) est pertinente.

Le tableau final (tableau 7.6, page suivante) reprend les seules fiches de recommandations estimées pertinentes et constitue l'aboutissement de la méthode. Ces fiches sont reproduites (à l'exception de leur partie explicative) en ANNEXE 5.

7.5. Evaluation globale

Nous ne nierons pas que la méthode du CEA nous a posé quelques difficultés, principalement au niveau de la compréhension de la démarche et de ses objectifs. Pourtant, il ne nous semble pas que les difficultés rencontrées proviennent de la méthode elle-même, mais plutôt du manque de clarté - et parfois de cohérence - de la documentation en notre possession [CEA]. Les principaux reproches que nous pourrions faire ici tiennent en quelques lignes:

- l'outil est incomplet: son développement, qui débuta à peu près à la même période que celui de la norme ITSEC (au début des années 1990), fut abandonné. Pourtant, la commission idoine du CEA avait précisément parmi ses objectifs le *positionnement par rapport au système européen d'évaluation de la sécurité des systèmes* ([CEA], page 9). Il n'est pas exclu d'imaginer que l'émergence de ces grandes méthodologies internationales, et surtout de leur volet d'assurance de certification[72], a rendu caducs les travaux du CEA;
- la documentation n'est pas toujours très claire; elle donne l'impression que la démarche elle-même n'était pas encore finie, ce qui est d'autant plus probable que le document en notre possession s'annonçait lui-même comme une *publication préalable*;
- illustration du point qui précède, l'existence de nombreuses contradictions - par exemple entre les différents tableaux de références croisées - qui sont parfois très perturbantes;

[72] Les méthodologies comme l'ITSEC contiennent un volet d'exigences d'assurance qui, si elles sont remplies, permettent la certification du niveau de sécurité du produit évalué par rapport à une échelle définie et reconnue internationalement.

- la démarche, peu formelle et parfois sibylline, laisse à chaque niveau une très large place à l'interprétation subjective, ce qui nous pousse à nous demander si en fin de compte l'auditeur ne pourrait pas en tirer exactement ce qu'il voudrait en tirer;

Tableau 7.6	**Sélection des fiches de recommandations.**			
1. - Mesures prioritaires (***)				
Type de Menace [73]	*Fiche*	*Importance*	*Niveau*	*Objet de la recommandation*
M4	20	***	R2	*(7.4.2.o)* Authentification et contrôle d'accès à granularité suffisamment fine; audit des transactions (7.4.2.c).
2. - Mesures secondaires (**)				
Type de Menace	*Fiche*	*Importance*	*Niveau*	*Objet de la recommandation*
E2	5	**	R2	*(7.4.2.p)* Analyse des risques: utilisation d'une méthode formelle reconnue (7.4.2.d).
E2	6	**	R1	*(7.4.2.q)* Procédures de sécurité: formalisation écrite (7.4.2.e).
E2	7	**	R3	*(7.4.2.r)* Audit: faire procéder à des tests d'intrusion (7.4.2.f)
M1	9	**	R2	*(7.4.2.s)* Bâtiments: compartimentage selon fonction des locaux, et contrôles d'accès (7.4.2.a).
E2	22	**	R3	*(7.4.2.t)* Sécurité IT: méthodologie rigoureuse (développement, réception, administration, contrôles) et chiffrement des données (7.4.2.g).
E2	27	**	R2	*(7.4.2.u)* Journalisation de la maintenance: évolutions et incidents (patches, versions, ...) (7.4.2.h).
1. - Mesures facultatives (*)				
Type de Menace	*Fiche*	*Importance*	*Niveau*	*Objet de la recommandation*
E2	1	*	R3	*(7.4.2.v)* Education: sensibilisation régulière de l'ensemble du personnel (7.4.2.i).
E2	4	*	R3	*(7.4.2.w)* Recensement et classification des objets; désignation d'un responsable et des procédures de sécurité (7.4.2.j).
M4	21	*	R2	*(7.4.2.x)* Journalisation: enregistrement, conservation et analyse de l'audit d'exploitation (activité) (7.4.2.k) dans le respect de notre besoin de confidentialité [G] (4.5.1.a).
E2	23	*	R2	*(7.4.2.y)* Documentation: sauvegarde et protection (7.4.2.l).
M4	26	*	R1	*(7.4.2.z)* Accès aux salles informatiques: limité au personnel nécessaire (7.4.2.m).
E2	28	*	R2	*(7.4.2.aa)* Sécurité de l'exploitation: suivi et contrôle d'exploitation (7.4.2.n).

- les 13 types de menaces[G], ainsi que les 28 fiches de recommandations, mériteraient davantage de développement. Avec notre petite application et nos 5 critères, nous avions déjà sélectionné 23 des 28 fiches existantes, avant de réduire ce nombre à 13. Clairement, nous serions probablement arrivés au même résultat en nous contentant de lire ces fiches une par une et de sélectionner celles qui nous paraissaient relevantes;
- M6 - qui nous avait déjà causé du souci au chapitre précédent - n'est tout simplement pas pris en considération ici. On se souviendra pourtant que M6 représentait 60% des pertes financières estimées consécutives à une atteinte au critère de confidentialité (6.4.2).

D'un autre coté, nous ne devons pas oublier que l'objectif du CEA était l'établissement d'une méthode simple d'évaluation - réalisée en premier rang par des non informaticiens - de systèmes existants en vue de proposer une couverture d'assurance. Cette mise au point effectuée, nous ne cacherons pas non plus que plusieurs éléments de l'approche du CEA nous ont séduits:

[73] Nous n'indiquons ici que le type de menace dont le niveau de gravité, supérieur, détermine le niveau de la recommandation à utiliser si disponible. En cas d'égalité de niveau, nous n'indiquerons que le type de menace qui aurait un impact sur le plus grand nombre de critères (tableau 7.5).

- le principe du questionnaire d'audit, qui permet très rapidement de mettre en évidence des choses vraiment importantes (surtout au niveau de la sécurité physique),
- le principe des fiches de recommandations (encore une fois, quelque chose de rapide et de pragmatique),
- la (relative) légèreté de l'ensemble qui devrait le rendre abordable rapidement par des petites structures et pour des petits projets et
- enfin - peut-être même surtout - ce concept de *phasing* qui établit une distinction entre l'importance et la perception de l'urgence: les recommandations provenant des fiches identifiées comme importantes ou efficaces (celles qui comportent davantage d'étoiles) sont à implémenter *en premier lieu*, quelle que soit notre perception de l'urgence qui nous pousserait au contraire à traiter en priorité les fiches destinées à palier les types de menaces[G] les plus graves (donc celles dont le niveau de recommandation est plus élevé)[74]. Si nous assimilons les types de menaces[G] à des *stresseurs* et les problèmes de sécurité à des situations de *stress*, il est amusant de se dire qu'une des caractéristiques habituelles des situations ou états de stress est précisément cette difficulté à établir la distinction entre ce qui est important et ce qui, même urgent, l'est moins.

En conclusion il nous semble que l'existence d'un outil de la catégorie de celui-ci, du fait de son utilité dans une niche bien particulière, est parfaitement justifiée; mais à la condition préalable d'en étoffer quelque peu le matériel[75] et d'en parfaire la mise au point.

[74] Ce qui n'empêche évidemment pas qu'une fiche de recommandations importante (***) soit à implémenter au niveau R3.

[75] Rappelons à ce sujet que seuls deux des trois niveaux du questionnaire ont été effectivement développés.

Chapitre 8 La suite d'EBIOS

8.1. Introduction

Nous avons déjà présenté la méthode EBIOS au chapitre 5 dans le cadre de l'expression des besoins de sécurité. Nous allons à présent poursuivre le travail, entrepris alors, par l'application des troisième et quatrième étapes de cette méthode que sont l'*étude des risques* et l'*identification des objectifs de sécurité.*

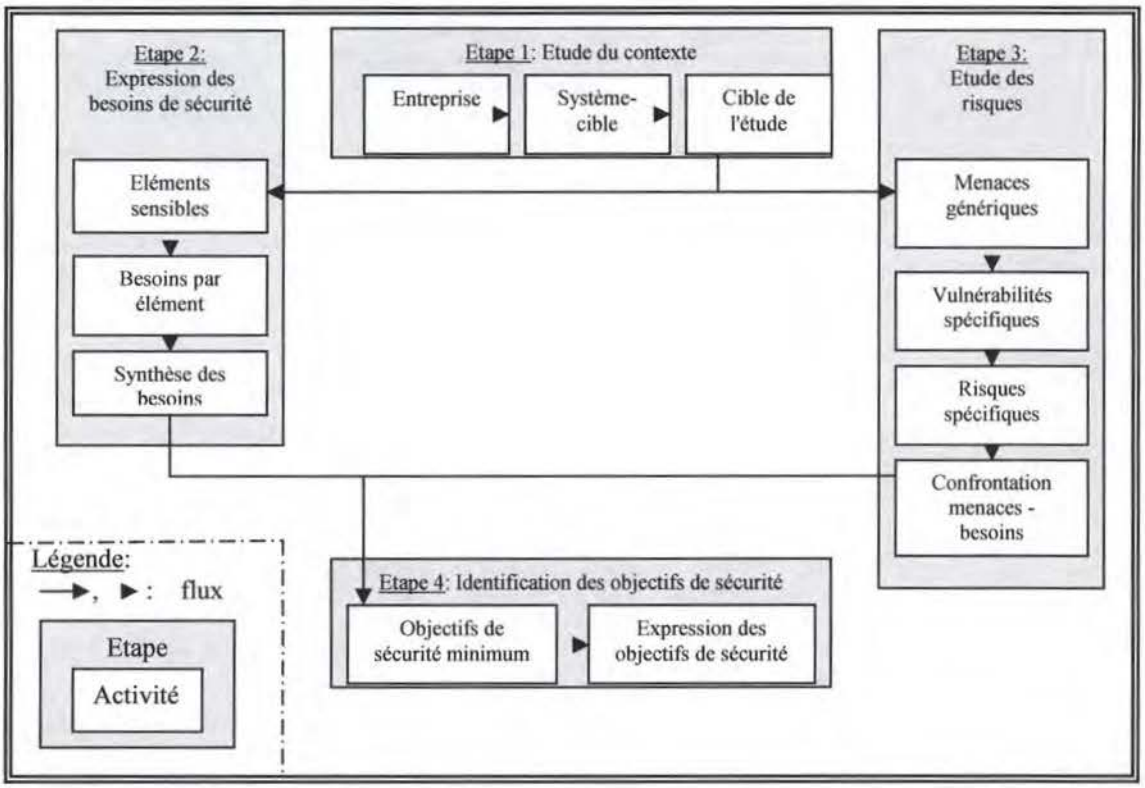


Figure 8.1: découpe complète de la méthode EBIOS en étapes et activités

Au cours de l'étape 3 (étude des risques[G]), nous aurons à sélectionner - sur base d'un catalogue - puis à croiser entre elles les menaces[G] génériques relevantes et les vulnérabilités[G] spécifiques liées à notre projet et à ses caractéristiques (principalement, les différentes entités préalablement identifiées). La mise en rapport d'une menace[G] et d'une (ou de plusieurs) vulnérabilité(s)[G] définira chacun de nos risques[G] spécifiques, risques[G] dont nous confronterons ensuite les menaces[G] desquelles ils découlent avec nos besoins de sécurité tels que nous les avons exprimés.

De cette confrontation naîtra, à l'étape 4, la liste de nos objectifs de sécurité minimum.

8.2. Etape 3: l'étude des risques

8.2.1. Présentation de l'étape

L'étape d'étude des risques[G] se décompose en quatre activités illustrées par la figure 8.1 ci-dessus.

L'*étude des menaces*[G] *génériques* consiste, sur base d'une liste de menaces[G] génériques (liste visant l'exhaustivité) à sélectionner celles dont la réalisation serait de nature à avoir un impact sur le SC. Dans un second temps, chaque menace[G] générique sera affectée d'une valeur de *sévérité* destinée à caractériser, si elle se réalisait, l'impact intrinsèque[76] de cette menace[G] sur le SC - et ce pour chacun des critères d'évaluation retenus.

Tableau 8.1	**Echelle de sévérité** (source: [EB-T])
Niveau	*Description*
0	Aucune conséquence
1	Conséquence faible
2	Perte moyenne
3	Perte importante
4	Perte complète

Les valeurs possibles de *sévérité* des menaces[G] génériques sont reprises au tableau 8.1. Le lecteur trouvera, en outre, la liste des menaces[G] génériques regroupées par thèmes en ANNEXE 6.

Pour chaque menace[G] générique retenue, l'étape d'*étude des vulnérabilités*[G] *spécifiques* consiste à sélectionner puis à valoriser les vulnérabilités[G] spécifiques qui sont à considérer. La sélection s'effectue sur base d'une liste des vulnérabilités[G] spécifiques associées à chaque menace[G] générique et regroupées par type d'entité concernée (les entités du SC figurent au tableau 5.4); la valorisation consiste à estimer au cas par cas la *faisabilité* (dans le cas d'une attaque) ou la *probabilité* (dans le cas d'un accident) qu'une menace[G] générique donnée puisse exploiter une vulnérabilité[G] spécifique pour chaque entité particulière. Cette estimation est établie sur base d'une échelle d'évaluation des menaces[G] en termes de faisabilité et de probabilité (tableau 8.2)

Tableau 8.2	**Echelles d'évaluation des menaces en termes de faisabilité (F) et de probabilité (P)** (source: [EB-T])	
Valeurs (F ou P)	*Signification en faisabilité (F)*	*Signification en probabilité (P)*
0	Infaisable	Improbable
0,25	Nécessiterait des moyens très importants et/ou des connaissances très élevées	Probabilité faible
0,5	Nécessiterait un certain niveau d'expertise et/ou du matériel spécifique	Probabilité moyenne
0,75	Réalisable avec des moyens standards et/ou avec des connaissances de base.	Probabilité forte
1	Réalisable par tout public.	Certaine

Le lecteur trouvera la liste (non exhaustive) des vulnérabilités[G] spécifiques proposée par EBIOS [EB-O] en ANNEXE 8.

Une fois les risques[G] génériques et les vulnérabilités[G] spécifiques sélectionnés, l'activité d'*étude des risques*[G] *spécifiques* consiste à croiser les résultats des deux premières activités pour en déduire une série de scénarii de risques[G] possibles. La valeur de *faisabilité* ou de *probabilité* associée à chaque risque[G] pourra être obtenue en calculant le produit des valeurs de *faisabilité* ou de *probabilité* liées à chaque vulnérabilité[G] exploitée dans le scénario considéré[77] *(8.2.1.a)*.

Pour terminer, l'étape de *confrontation des risques*[G] *aux besoins* consiste à mettre en relation d'une part les risques[G] spécifiques (résultat de l'activité précédente) et d'autre part les fonctions et catégories d'informations sensibles de l'autre, cette mise en relation s'effectuant par l'intermédiaire des entités qu'affectent les premiers et qu'utilisent les seconds. Pour ce faire, une fiche est établie pour chaque fonction ou catégorie d'information sensible, sur laquelle sont reprises toutes les menaces[G] qui s'appuient sur des vulnérabilités[G] affectant les entités qu'utilise cette fonction ou catégorie d'informations: l'impact réel de la menace[G] pour chaque critère (disponibilité[G], intégrité[G], confidentialité[G], imputabilité[G] et écologie[G]) sera égal à 0 si la menace[G] n'affecte pas ce critère (sévérité nulle); dans le cas contraire (sévérité non nulle) l'impact réel sera égal à la sensibilité de la fonction ou de la catégorie d'informations. Une fois sélectionnés, les risques[G] dont l'impact correspond à une de nos sensibilités (ou besoins de sécurité) sont regroupés par

[76] La sévérité de la menace est réputée indépendante de la sensibilité des fonctions et informations du SC: on peut donc avoir un perte totale (sévérité 4) en confidentialité même si la nature des informations concernées n'est pas confidentielle.

[77] Par exemple la faisabilité (F) qu'un technicien externe puisse *pénétrer dans la site* (F1) et *piéger un téléphone* (F2) vaudra F1 * F2.

menace[G], affectés à une catégorie (selon le niveau estimé de l'origine du risque[G] ou de l'agresseur potentiel[78]) et le type de la ou des contre-mesure(s) est arrêté *(8.2.1.b)*.

8.2.2. Etape 3 - Activité 1: étude des menaces génériques

La fiche de sélection des menaces[G], document final de cette première activité représenté, reprend pour chaque menace[G] générique (ANNEXE 6) retenue les informations suivantes:

- l'identification de la menace[G] (son numéro de code et son nom);
- la cause de la menace[G]:
  - 'F' pour une cause *fortuite* (accidentelle), 'V' pour une cause *volontaire* (intentionnelle);
- l'origine de la menace[G]:
  - 'L' pour *ludique*, 'A' pour *avide*, 'S' pour *stratégique* et 'T' pour *terroriste*;
- les critères affectés et la valeur estimée de sévérité (tableau 8.1):
  - disponibilité[G], confidentialité[G], imputabilité[G], écologie[G] et intégrité[G];
- un (lien vers un) commentaire éventuel.

Comme d'habitude, l'établissement des valeurs de sévérité fait appel à une large part de subjectivité, et constitue un exercice difficile et incertain. Comment, par exemple, estimer entre 0 et 4 (tableau 8.1) la sévérité d'une atteinte à la disponibilité[G] ou à l'intégrité[G] du SC que représenterait une menace[G] générique comme *dysfonctionnement logiciel*[79] ? Encore une fois, il nous semble que la qualité du résultat devrait être proportionnelle au nombre de personnes participant à l'évaluation.

Avant de nous lancer dans cet exercice il nous paraît opportun - pour garder à ce chapitre des dimensions raisonnables - d'introduire quelques nouvelles hypothèses simplificatrices que voici:

- *(8.2.2.a)* l'entreprise n'étant pas une cible prestigieuse et ne détenant aucun secret militaire ni technologique, les moyens mis en oeuvre pour une attaque à motivation avide seront probablement proportionnels au gain escompté; nous avons donc considéré que toute menace[G] volontaire qui impliquerait la mise en place d'éléments matériels et/ou coûteux ne serait pas retenue[80];
- *(8.2.2.b)* pour les mêmes raisons, nous ne considérerons pas les possibilités de sabotage matériel;
- *(8.2.2.c)* pour les mêmes raisons, les menaces[G] liées à l'écoute passive seront évaluées sur base du matériel existant seulement (machines connectées);
- *(8.2.2.d)* comme en tout état de cause nous ne disposons d'aucun moyen d'action sur les environnements physiques des sous-systèmes distants, nous ne considérerons plus les menaces[G] physiques (y compris les pertes d'alimentation électrique) pesant sur ces environnements[81].

Le résultat de cette activité est illustré par la fiche de sélection des menaces[G] génériques du sous-système serveur ci-dessous (tableau 8.3). Les fiches équivalentes pour le sous-systèmes local et distants figurent en ANNEXE 7.

Tableau 8.3	**Fiche de sélection des menaces génériques pour E_S_SITE (site 'serveur')**											
Menaces génériques	*F*	*V*	*L*	*A*	*S*	*T*	*D*	*C*	*W*	*I*	*E*	*Commentaire*
1- INCENDIE	Menace non retenue (5.2.3.4.b)											
2- DÉGÂT DES EAUX	Menace non retenue (manque de pertinence)											
3- POLLUTION	Menace non retenue (manque de pertinence)											
4- ACCIDENTS MAJEURS	Menace non retenue (manque de pertinence)											
5- PHENOMENE CLIMATIQUE	Menace non retenue (manque de pertinence)											
6- PHENOMENE SISMIQUE	Menace non retenue (manque de pertinence)											
7- PHENOMENE VOLCANIQUE	Menace non retenue (manque de pertinence)											

[78] Les 3 niveaux sont *élémentaire* (risque aléatoire), *moyen* (agresseur à ressources limitées) et *élevé* (agresseur disposant de beaucoup de moyens).

[79] Menace générique numéro 26, ANNEXE 6.

[80] Il s'agit malgré tout d'une simplification discutable, non du fait de l'entreprise elle-même mais plutôt par rapport au profil de certains de ses clients ASP.

[81] L'impact d'un sinistre de nature physique qui frapperait un sous-système distant n'affecterait d'ailleurs la plupart du temps que le critère de disponibilité pour un ou deux utilisateurs.

Tableau 8.3 (suite)	**Fiche de sélection des menaces génériques pour E_S_SITE (site 'serveur')**											
Menaces génériques	*F*	*V*	*L*	*A*	*S*	*T*	*D*	*C*	*W*	*I*	*E*	*Commentaire*
8- PHENOMENE METEOROLOGIQUE	Menace non retenue (manque de pertinence)											
9- CRUE	Menace non retenue (manque de pertinence)											
10- DÉFAILLANCE DE LA CLIMATISATION	Menace non retenue (5.2.3.4.b)											
11- PERTE D'ALIMENTATION ÉNERGÉTIQUE	Menace non retenue (5.2.3.4.b)											
12- PERTE DES TÉLÉCOMMUNICATIONS	X	X	X				3					Voir [82].
13- RAYONNEMENTS ELECTROMAGNETIQUES	Menace non retenue (manque de pertinence)											
14- RAYONNEMENTS THERMIQUES	Menace non retenue (manque de pertinence)											
15- IMPULSIONS ELECTROMAGNETIQUES	Menace non retenue (manque de pertinence)											
16- INTERCEPTION DE SIGNAUX PARASITES	Menace non retenue (manque de pertinence)											
17- ESPIONNAGE A DISTANCE	Menace non retenue (manque de pertinence)											
18- ÉCOUTE PASSIVE		X		X				3				Voir [83].
19- VOL DE SUPPORTS OU DE DOCUMENTS		X		X				3				Voir [84].
20- VOL DE MATÉRIELS		X		X			4	3				Voir [85] [86] [87].
21- DIVULGATION INTERNE	Menace non retenue (5.2.3.4.a).											
22- DIVULGATION EXTERNE	Menace non retenue (5.2.3.4.a).											
23- PANNE MATÉRIELLE	X						4					Voir [88].
24- DYSFONCTIONNEMENT MATÉRIEL	X						2					Médiane.
25- SATURATION DU MATÉRIEL	X	X	X				4					Voir [89].
26- DYSFONCTIONNEMENT LOGICIEL	X						2	2	2	2	3	Voir [90].
27- DESTRUCTION DE MATÉRIELS	Menace non retenue (le matériel n'est pas fragile de nature)											
28- ATTEINTE A LA MAINTENABILITE DU SI	Menace non retenue											
29- INFORMATIONS SANS GARANTIE DE L'ORIGINE	Menace non retenue (5.2.3.4.a).											
30- PIEGEAGE DU MATERIEL	Menace non retenue (5.2.3.4.a).											
31- UTILISATION ILLICITE DU MATÉRIEL		X	X	X			2	3	3	3	4	Voir [91].
32- ALTÉRATION DU LOGICIEL		X	X	X			3			4		Bombe, virus, vers, ...
33- PIÉGEAGE DU LOGICIEL		X	X	X			2	3	3	4	3	Voir [92].

[82] Perte totale mais probablement de durée limitée (SLA de l'ISP) en disponibilité[G].
[83] A priori, la perte en confidentialité [G] impliquerait I_COMM et I_PROFIL (5.2.4.2.f) pour tous les utilisateurs.
[84] Seules catégories d'informations persistantes éventuellement exploitables: I_AUTH et I_PROFIL, pour plusieurs utilisateurs.
[85] En cas de vol du serveur, perte totale de longue durée (pas de serveur backup) en disponibilité [G].
[86] Seules catégories d'informations persistantes éventuellement exploitables: I_AUTH et I_PROFIL, pour plusieurs utilisateurs.
[87] Atteinte en confidentialité[G] uniquement en cas de vol du serveur du SC lui-même (5.2.4.2.c).
[88] En cas de vol du serveur, perte totale de longue durée (pas de serveur backup) en disponibilité [G].
[89] Engorgement (atteinte accidentelle mais structurelle) ou parasitage intense et continu (atteinte volontaire): perte totale de longue durée en disponibilité [G].
[90] Médiane, sauf écologie[G] (4.6.6.b) (4.6.6.c).
[91] Permettrait la consultation et l'altération des catégories d'informations I_AUTH, I_PROFIL et I_PARAM;
[92] Cheval de Troie, trappe, canal caché: impact en intégrité [G] (du logiciel et) des données non persistantes seulement, la gestion des données persistantes (enrôlement[G] et maintenance) s'effectuant directement sur le serveur (4.4.3.d) et indépendamment du SC (4.4.3.d) (4.4.3.g).

Tableau 8.3 (suite)	**Fiche de sélection des menaces génériques pour E_S_SITE (site 'serveur')**											
Menaces génériques	*F*	*V*	*L*	*A*	*S*	*T*	*D*	*C*	*W*	*I*	*E*	*Commentaire*
34- COPIE FRAUDULEUSE DE LOGICIEL	Menace non retenue (5.2.3.4.a)..											
35- UTILISATION DE LOGICIELS FRAUDULEUX	Menace non retenue (5.2.3.4.a)..											
36- ALTÉRATION DES DONNÉES		X	X	X			2	4	4	4	4	Voir [93].
37- ERREUR DE SAISIE	X						2	2	3		4	Voir [94].
38- ERREUR D'UTILISATION	Menace non retenue (absence d'utilisateur).											
39- ABUS DE DROIT	Menace non retenue.											
40- USURPATION DE DROIT		X		X			2	2	4	2		Voir [95].

8.2.3. Etape 3 - Activité 2: étude des vulnérabilités spécifiques

Nous avons ensuite procédé, pour chaque menace[G] générique retenue et chaque entité du SC concernée, à l'évaluation des vulnérabilités[G] spécifiques (ANNEXE 8) susceptibles de permettre à cette menace[G] de se réaliser. La question à laquelle chacune de ces évaluations répond est donc la suivante: *quelle est la probabilité ou la faisabilité que la vulnérabilité[G] spécifique VS liée à l'entité E du SC permette à la menace[G] générique MG de se réaliser (8.2.3.a) ?*

Notre devoir de réserve[96] ne nous permettant toutefois pas d'envisager toutes les vulnérabilités[G] spécifiques proposées (notamment la plupart de celles qui sont liées aux entités *personnels*, *sites* ou *organisation*), nous sommes partis de l'hypothèse que lorsqu'une de ces entités sensibles était considérée, la réponse implicite à la question précitée était "0" (faisabilité ou probabilité nulle - Cfr. tableau 8.2). Pour faciliter notre évaluation, nous avons donc établi ou complété les règles suivantes:

- *(8.2.3.b)* sauf exception, l'évaluation des vulnérabilités[G] spécifiques par rapport aux entités *personnels*, *sites* ou *organisation* sera toujours égale à "0" [97];
- *(8.2.3.c)* les vulnérabilités[G] spécifiques dont l'ensemble des évaluations par rapport à toutes les entités considérées vaudront "0" ne seront pas retenues;
- *(8.2.3.d)* lorsque ce sera relevant, le niveau de faisabilité "0,75" sera réputé correspondre aux capacités d'une personne un peu avertie et disposant de quelques connaissances techniques (pas de connaissance approfondie au niveau logiciel);
- *(8.2.3.e)* lorsque ce sera relevant, le niveau de faisabilité "0,50" sera réputé correspondre aux capacités d'un informaticien débrouillard;
- *(8.2.3.f)* lorsque ce sera relevant, le niveau de faisabilité "0,25" sera réputé correspondre aux capacités d'un véritable expert;
- *(8.2.3.g)* étant donné que nous n'avons aucun moyen de contrôle sur aucun élément des sites *distants* (E_D_SITE), l'évaluation de la facilité à pénétrer ces sites sera évaluée à "1" (surtout tenant compte de l'existence d'ordinateurs portables).
- *(8.2.3.h)* étant donné que nous n'avons aucun moyen de contrôle sur aucun élément des sites *distants* (E_D_SITE), l'évaluation de la facilité à pénétrer les systèmes qui y résident sera évaluée à "0,75".
- *(8.2.3.i)* en cas de panne matérielle du serveur du SC, la réparation n'est pas réputée faisable endéans les 26 heures (non respect du SLA);
- *(8.2.3.j)* en cas de panne matérielle au niveau des serveurs des dispositifs de protection logique ou d'un élément du LAN, la réparation ou le remplacememnt est réputé faisable endéans les 26 heures (respect du SLA, tenant compte d'une panne annuelle seulement);

---

[93] Une atteinte à l'intégrité [G] des données (I_AUTH, I_COMM, I_PROFIL I_CODBIN et I_PARAM) aurait des conséquences en disponibilité [G] pour tous les utilisateurs (hypothèse: durée limitée), en confidentialité[G] pour tous les utilisateurs, en imputabilité[G] (4.5.1.h) (4.5.1.j) pour tous les utilisateurs et en écologie (4.3.3.g) (4.3.3.h). Notons que EBIOS semble ne considérer ici que les seules données transmises, ce qui n'est pas notre approche.

[94] Principalement en cas d'erreur de paramétrage du SC (4.3.3.g) (4.3.3.h) ou lors de l'enrôlement [G] des utilisateurs.

[95] Imputabilité: rejeu (4.5.1.h) ou attaque du style *man in the middle*[G] (4.5.1.j).

[96] Vulnérabilité spécifique associée au personnel.

[97] D'où disparition des menaces 21 et 22 (divulgation) de E_D_SITE, et si nous ne l'avions déjà fait cela nous aurait permis également d'éliminer d'autres menaces liées au site ou à l'organisation comme *incendie* ou *alimentation électrique*.

- *(8.2.3.k)* dans le contexte de l'établissement de ces tableaux, nous considérons que le terme *modifier* signifie *introduire une modification fonctionnelle ou porteuse de sens*, et non simplement *brouiller*.

Afin d'illustrer cette étape, nous avons repris au tableau 8.4 un extrait d'une de ces grilles d'évaluation des vulnérabilités[G] spécifiques dont le lecteur trouvera l'intégralité en ANNEXE 9. Dans ces grilles, chaque vulnérabilité[G] est identifiée par un code unique qui figure à l'ANNEXE 8, code qui commence toujours par le numéro de la menace[G] (ANNEXE 6).

Tableau 8.4	**Vulnérabilités spécifiques (E_S_SITE) - extrait du tableau A9.1 (ANNEXE 9)**				
Menaces et vulnérabilités associées retenues avec estimation de faisabilité / probabilité par type d'entité	*LAN*	*WAN[98] (LLine)*	*WAN[99] (INET)*	*E_S_ SITE*	*E_S_ ADMIN*
12- Pertes des télécommunications					
12RE1- Le réseau externe peut être soumis à des défaillances graves		0,00	0,50		
12RE2- Le réseau externe peut être détruit		0,25[100]	0,00[101]		
18- Ecoute passive					
18RI1- Matériel ayant des éléments permettant l'écoute passive	0,75				
18RE1- Réseau ayant des caractéristiques permettant l'écoute passive		0,50	0,50		
18S3- Facilité de pénétrer les locaux				0,50	
19- Vol de supports ou de documents					
19S2- Facilité de pénétrer le site				0,50	
19P1- Manque de vigilance					0,25

8.2.4. Etape 3 - Activité 3: étude des risques spécifiques

Nos vulnérabilités[G] sont connues et leur faisabilité / probabilité de réalisation estimée: il reste maintenant à imaginer les différents scénarii de risques[G] possibles. Le tableau 8.5 illustre cette activité en reprenant une partie de ces scénarii imaginés avec, chaque fois, l'identification de la menace[G] générique, la description du scénario, le rappel de la sévérité de la menace[G] [102] et la valeur finale de faisabilité / probabilité résultant de la combinaison des valeurs élémentaires estimées pour chaque vulnérabilité[G] (8.2.1.a). Le lecteur trouvera en ANNEXE 10 l'intégralité des grilles d'évaluation des risques[G] spécifiques.

Tableau 8.5	**Risques spécifiques (E_S_SITE) - extrait du tableau A10.1 (ANNEXE 10)**						
MENACES GENERIQUES	*RISQUES SPECIFIQUES*	*D*	*C*	*W*	*I*	*E*	*F/P*
12- PERTE DES TÉLÉCOMMUNICATIONS	Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)	3					0,50
	Destruction accidentelle de la liaison à l"Internet (boucle locale): 12RE2(LLINE)	3					0,25
18- ÉCOUTE PASSIVE	Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN[103]: 18RI1*18S3		3				0,50 * 0,75
	Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)		3				0,50
19- VOL DE SUPPORTS OU DE DOCUMENTS	Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe des supports ou des documents: 19S2*19P1		3				0,50 *0,25

A la fin de cette activité, nous nous retrouvons avec près de 75 scénarii de risques[G] différents, ce qui est beaucoup dans le contexte de ce travail tel que décrit auparavant (5.1.1). Nous avons donc imaginé la méthode relativement arbitraire suivante pour diminuer sensiblement ce nombre de cas de figure à considérer:

[98] LLine: ligne louée.
[99] INET: Internet
[100] Un engin de génie civil pourrait trancher la boucle locale (impact sur la ligne louée comme sur la ligne backup)
[101] Selon un de ses principes fondateurs.
[102] Ces valeurs de sévérité, estimées globalement par menace au tableau 8.3 illustrant l'ANNEXE 7, sont parfois revues à la baisse pour certains scénarii spécifiques.
[103] Comme nous avons exclu l'ajoût de matériel, et à moins d'un enregistrement sur une station locale avec écoute différée, cette écoute aurait lieu en dehors des heures de travail du site E_S_SITE.

- dans les grilles de l'ANNEXE 10, nous remplaçons chaque valeur de sévérité par le produit de cette valeur avec le contenu de la colonne de faisabilité / probabilité, ce qui nous donne pour chaque critère une nouvelle valeur que nous nommerons la *sévérité pondérée*;
- nous conserverons les seuls scénarii de risques[G] qui rempliront une des conditions suivantes:
  - avoir au moins une valeur de sévérité pondérée supérieure ou égale à 1,00,
  - avoir au moins deux valeurs de sévérité pondérée supérieures ou égales à 0,75,
  - avoir au moins trois valeurs de sévérité pondérée supérieures ou égales à 0,50 ou
  - avoir au moins quatre valeurs de sévérité pondérée supérieures ou égales à 0,25.

Les lignes de l'ANNEXE 10 qui figurent en caractères gras correspondent aux scénarii répondant à au moins un de ces critères; les autres ne seront plus pris en considération.

8.2.5. Etape 3 - Activité 4: Confrontation des menaces aux besoins

Chacun des risques[G] spécifiques sélectionnés (8.2.4) exploite donc une ou plusieurs vulnérabilité(s)[G] spécifique(s) (8.2.3). Or, chacune de ces vulnérabilités[G] spécifiques est associée à une ou plusieurs entités du SC (tableau 8.4 et ANNEXE 9), lesquelles entités sont exploitées par certaines fonctions ou catégories d'informations du SC. Nous pouvons donc établir la relation entre la menace[G] à l'origine du risque[G] d'une part et la fonction ou catégorie d'informations d'autre part de la manière suivante: la menace[G] générique *MG* aura un impact réel *IR* sur le critère *C* de la fonction ou catégorie d'informations *FCI* si les trois conditions suivantes sont réunies:

- *MG* et *FCI* doivent concerner au moins une entité *E* commune,
- la sévérité de *MG* par rapport à *C* n'est pas nulle et
- la sensibilité de *FCI* par rapport à *C* n'est pas nulle.

Si ces trois conditions sont remplies, la valeur de l'impact réel *IR* de *MG* par rapport au critère *C* de *FCI* sera égale à la sensibilité de *FCI* par rapport à *C (8.2.5.a)*.

Le lecteur trouvera en ANNEXE 11 les grilles exprimant les relations entre menaces[G] génériques et entités du SC, grilles sur base desquelles les fiches de confrontation des menaces[G] aux besoins sont élaborées. Au vu de ces grilles, le lecteur constatera rapidement que les entités *SITE*[104] sont concernées par la majorité des risques[G] sous l'angle de la vulnérabilité[G] *pénétration du site*; pour alléger notre démarche nous avons donc décidé de ne plus en tenir compte ici, mais de marquer cette observation d'une pierre blanche pour usage ultérieur *(8.2.5.b)*.

Le tableau 8.6 ci-dessous reprend à des fins d'illustration une des fiches de confrontation des risques[G] aux besoins; ces fiches figurent en ANNEXE 12.

Tableau 8.6	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_PARAM*						*D*	*C*	*W*	*I*	*E*
							2		*3*	*3*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**2**		**3**	**3**	
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**2**		**3**	**3**	
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**2**		**3**	**3**	

Reste maintenant à établir les fiches de synthèse qui regroupent ces risques[G] par menaces[G], définissent leur catégorie et permettent de choisir le type de contre-mesures (8.2.1.b). Lors du regroupement des risques[G] par menace[G] au départ des fiches de confrontation que nous venons d'élaborer, nous éliminerons les doublons (mêmes risques[G] impliquant plusieurs entités différentes) ainsi que les risques[G] n'ayant pas d'impact réel, et

[104] E_S_SITE, E_L_SITE et E_D_SITE.

regrouperons également certains risques[G] similaires sous une même dénomination plus générique mais malgré tout suffisamment précise[105].

Les tableaux 8.7 à 8.9 ci-dessous représentent nos fiches de synthèse, documents finaux de cette activité.

Tableau 8.7 Fiche de synthèse des risques pour E_S_SITE

MG	*Risques majeurs pour E_S_SITE*	*Impact réel*					*Cat.*	*Type m.*	
		D	*C*	*W*	*I*	*E*		*T*	*NT*
12	S1- Défaillances graves dans le fonctionnement et les performances de l'Internet	2					1		X
18	S3+S4 Ecoute passive au niveau du LAN ou du WAN		3				2	X	X
20	S6+S7 Vol du serveur d'application ou d'un élément du LAN	2	3				1		X
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	2					1	X	
25	S15- Attaque de type DOS depuis l'extérieur saturant la connexion WAN	2					2	X	
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC	2	3	3	3	4	1		X
36	S31+S32 Modification des données transitant sur le LAN ou le WAN (attaque type *man in the middle*)	2	3	3	2		3	X	
36	S33- Compromission logique totale du serveur du SC	2	3	3	3	4	3	X	X

Tableau 8.8 Fiche de synthèse des risques pour E_L_SITE

MG	*Risques majeurs pour E_L_SITE*	*Impact réel*					*Cat.*	*Type m.*	
		D	*C*	*W*	*I*	*E*		*T*	*NT*
18	L2- Ecoute passive au niveau du LAN		3				2	X	X
20	L3+L4 Vol de tous les postes clients ou d'un élément du LAN	2					1		X
26	L10- Dysfonctionnement logiciel de l'ensemble des postes clients	2	3	3	2		1	X	
31	L12- Utilisation illicite du matériel	2	3	3	2		1		X
32	L13- Infection par vers ou virus depuis lInternet	2			2		1	X	X
32	L15- Effacement de fichiers ou de programmes des postes clients	2			2		2	X	
33	L16-+L17 Piégeage des postes clients,ou implantation de programmes pirates sur les poste clients	2	3	3	2		2	X	
33	L18- Piégeage du logiciel en phase de développement sur le poste du développeur	2	3	3	2	4	2	X	
38	L20- Absence de l'utilisateur après authentification	2	3	3			1		X

Tableau 8.9 Fiche de synthèse des risques pour E_D_SITE

MG	*Risques majeurs pour E_D_SITE*	*Impact réel*					*Cat.*	*Type m.*	
		D	*C*	*W*	*I*	*E*		*T*	*NT*
26	D9- Dysfonctionnement logiciel du (des) poste(s) client(s)	2	3	3	2		1	X	
31	D10- Consommation abusive des ressources du réseau par l'utilisation du (des) poste(s) client(s) à des fins non professionnelles	2	3	3			1		X
32	D12- Infection du (des) poste(s) client(s) par vers ou virus depuis lInternet	2			2		1	X	X
32	D13+D14- Effacement ou modification de fichiers ou d'applications du (des) poste(s) client(s)	2			2		2	X	
33	D15+D16 Piégeage du (des) poste(s) client(s) ou implantation de programmes pirates sur le (les) poste(s) client(s)	2	3		2		2	X	
38	D18- Absence de l'utilisateur après authentification		3	3			1		X

[105] Lorsque plusieurs risques sont regroupés en un seul, les valeurs d'impact réel par critère qui en résultent correspondent à ce que donnerait une fonction *maximum* appliquée aux impacts réels des risques avant regroupement.

8.3. Etape 4 - Identification des objectifs de sécurité

8.3.1. Présentation de l'étape

La dernière étape de ce long processus consiste à identifier nos objectifs (exigences) de sécurité sur base des risques[G] identifiés.

Dans un premier temps, les objectifs de sécurité minimum sont déterminés en identifiant la *classe de fonctionnalité ITSEC*[106] [EB-O] qui se rapproche le plus de notre SC; cette étape de sélection, qui n'offre guère d'intérêt particulier, s'effectue simplement à partir d'une grille dans laquelle on entre avec des informations comme la sensibilité maximale des informations et d'où on peut ressortir avec une ou plusieurs classes de fonctionnalités[107].

Enfin, la deuxième et tout dernière activité consiste à étoffer ces objectifs minimum,éventuellement à partir d'autres sources, en se basant plus directement sur les fiches de synthèse des risques[G] (tableaux 8.7 à 8.9). L'évaluateur peut alors rédiger le rapport final selon la forme qui convient le mieux à l'outil ou à la démarche qui suivra EBIOS[108] (voir ANNEXE 1).

8.3.2. Etape 4 - Activité 1: Choix des objectif de sécurité minimum

Le profil de notre SC nous a conduit à la sélection de la classe de fonctionnalité ITSEC *F-C2* que le lecteur trouvera in extenso à l'ANNEXE 13. Sur base de cette classe de fonctionnalités, qui se caractérise notamment par un modèle de contrôle d'accès discrétionnaire[G] et dont les prescriptions doivent être évaluées en fonction de notre contexte particulier, nous pouvons d'ores et déjà arrêter les objectifs de sécurité minimum suivants:

- *(8.3.2.a)* le système doit identifier et authentifier de façon unique les utilisateurs;
- *(8.3.2.b)* aucune autre interaction avec le système ne doit être possible sans une identification[G] et une authentification[G] préalables réussies;
- *(8.3.2.c)* pour chaque interaction entre un utilisateur et le système, le système doit pouvoir établir l'identité de l'utilisateur;
- *(8.3.2.d)* le système doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux;
- *(8.3.2.e)* il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet;
- *(8.3.2.f)* il doit être possible de limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas l'objet;
- *(8.3.2.g)* il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de l'utilisateur individuel;
- *(8.3.2.h)* il ne doit pas être possible à quelqu'un qui n'est pas utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet;
- *(8.3.2.i)* l'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès;
- *(8.3.2.j)* seuls des utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants;
- *(8.3.2.k)* lors de toute tentative par des utilisateurs ou groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, le système doit vérifier la validité de la demande;
- *(8.3.2.l)* les tentatives d'accès non autorisées (8.3.2.k) doivent être rejetées;

[106] Les *classes de fonctionnalités ITSEC* sont inspirées notamment des classes TCSEC [TCSEC].

[107] En réalité, ce processus est à appliquer pour chacun des critères de Disponibilité, Confidentialité et Intégrité avec chaque fois une grille différente. De chaque grille on peut ressortir avec 0 ou 1 classe(s) de fonctionnalités, ce qui nous donne au total entre 0 et 3 classes sélectionnées.

[108] La documentation EBIOS contient quelques indications sur ce qu'il convient de faire et la manière de procéder en fonction de la suite réservée à cette étude de risques.

- *(8.3.2.m)* le SC doit comporter un composant d'imputation qui soit capable d'enregistrer toutes les demandes d'identification[G] et d'authentification[G] avec toutes les informations relevantes par rapport au SC, à son utilisation et à ses contraintes;
- *(8.3.2.n)* le SC doit comporter un composant d'imputation qui soit capable d'enregistrer tous les événements *début de communication* avec les informations relevantes par rapport au SC, à son utilisation et à ses contraintes;
- *(8.3.2.o)* le SC doit comporter un composant d'imputation qui soit capable d'enregistrer tous les événements *fin de communication* avec les informations relevantes par rapport au SC, à son utilisation et à ses contraintes;
- *(8.3.2.p)* les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation;
- *(8.3.2.q)* il doit exister des outils pour examiner et maintenir les fichiers d'imputaton et ces outils doivent être documentés;
- *(8.3.2.r)* les outils d'analyse des fichiers d'imputation doivent permettre d'y effectuer des recherches sélectives.

8.3.3. Etape 4 - Activité 2: Expression des objectifs de sécurité

Aux objectifs minimum de sécurité énoncés ci-dessus, les éléments déjà connus de notre SC et les risques[G] identifiés (tableaux 8.7 8.9) nous permettent d'ajouter les exigences suivantes:

- *(8.3.3.a)* les sous-systèmes serveur et local devront faire l'objet d'une réévaluation des mesures techniques et procédurales de compartimentage et de protection contre l'intrusion (8.2.5.b) et le vol (menace[G] générique 20, tableaux 8.7 et 8.8). Cette exigence, principalement organisationnelle ou de nature physique, est citée ici par souci de complétude mais sort du cadre de ce document;
- *(8.3.3.b)* des procédures adéquates doivent être établies, documentées et distribuées pour qu'un problème de défaillance dans le fonctionnement et les performances de l'Internet qui altérerait la bonne exploitation du SC ne mette pas en cause la synergie entre les employés distants, le support des clients ni la réputation de l'entreprise. Cette exigence, principalement de nature organisationnelle, est citée ici par souci de complétude mais sort du cadre de ce document (menace[G] générique 12, tableau 8.7);
- *(8.3.3.c)* par rapport aux menaces de panne matérielle (menace[G] générique 23, tableau 8.7), une protection efficace consisterait à prévoir une redondance matérielle et la disponibilité[G] rapide d'un technicien (4.3.3.b). Ici aussi comme au paragraphe (4.3.3), on peut se demander si le coût d'une telle mesure de protection n'est pas disproportionné par rapport à l'impact estimé et aux ressources disponibles (1.2.3.b);
- *(8.3.3.d)* les menaces d'écoute passive (menace[G] générique 18, tableaux 8.7 et 8.8) devront être parées par l'utilisation du chiffrement systématique des communications, protégeant tant le contenu de conversations que l'identité des participants;
- *(8.3.3.e)* les menaces[G] d'attaque logique de type *DoS*[G] visant à saturer la bande passante disponible vers l'Internet (menace[G] générique 25, tableau 8.7) sont du ressort de la configuration des dispositifs de protection logique de l'entreprise et sortent du cadre de document ;
- *(8.3.3.f)* les menaces[G] de dysfonctionnement logiciel (menace[G] générique 26, tableaux 8.7 à 8.9) sont préoccupantes et nous obligent à considérer :
  - une procédure stricte de conception et développement, ou de réception et mise en quarantaine, des applications en vue de leur qualification avant déploiement;
  - le besoin d'un administrateur compétent pour assurer la configuration du SC et
  - le besoin de documentation technique ;
- *(8.3.3.g)* les menaces d'attaque logique de type *Man in the Middle*[G] (menace[G] générique 36, risques[G] S31+S32, tableau 8.7) doivent être parées par des mesures appropriées de chiffrement;
- *(8.3.3.h)* les menaces[G] de compromission logique totale du serveur du SC (menace[G] générique 36, risque[G] S23, tableau 8.7) doivent être parées par des mesures combinées d'accès physique (8.3.3.a), de protection logique externe (5.2.3.4.c) et de *host security*[109];
- *(8.3.3.i)* la menace[G] d'utilisation illicite du matériel (menace[G] générique 31, tableaux 8.8 et 8.9) doit être parée par des mesures organisationnelles qui sortent du cadre de ce document. A noter

[109] Malgré la protection externe assurée par les dispositifs de protection logique de l'entreprise, le serveur d'application du SC doit lui-même assurer sa propre sécurité, c'est-à-dire ne pas considérer l'environnement extérieur immédiat comme exempt de risque (même si nous considérons que c'est normalement le cas comme indiqué pour l'entité E_S_LAN au tableau 5.4).

toutefois que par hypothèse sur les employés (environnements E_S_SITE et une partie des E_D_SITE), cette menace[G] est normalement inexistante (5.2.3.4.b) ;

- *(8.3.3.j)* la menace[G] d'infection par un vers ou un virus (menace[G] générique 32, tableaux 8.8 et 8.9) doit être contrée par les mesures techniques adéquates, combinées à des mesures organisationnelles (convaincre d'appliquer les mesures techniques pour chaque sous-système distant ou E_D_SITE) ;
- *(8.3.3.k)* les menaces[G] d'altération ou de piégeage du logiciel (menaces[G] génériques 32 et 33, tableaux 8.8 et 8.9) doivent être contrées par le même genre de mesures que celles envisagées face à la menace[G] de compromission logique totale du serveur du SC (8.3.3.h) ;
- *(8.3.3.l)* les menaces[G] liées à des erreurs d'utilisation (menace[G] générique 38, tableaux 8.8 et 8.9) seront contrées par des mesures organisationnelles ainsi que par la nécessaire documentation et formation des utilisateurs. A noter toutefois que par hypothèse sur les employés (environnements E_S_SITE et une partie des E_D_SITE), cette menace[G] est normalement inexistante (5.2.3.4.b).

8.4. Conclusions

Conceptuellement, la démarche EBIOS peut se résumer aux quatre phases principales que constituent:

- l'identification des fonctions (tableau 5.2), catégories d'informations (tableau 5.2) et entités du SC (tableau 5.4), avec quantification de la sensibilité de chaque fonction et catégorie d'informations sensibles à l'étape 2 (tableau 5.10):
- l'identification des relations entre entités du SC d'une part et les fonctions ou catégories d'informations d'autre part (tableau 5.5);
- l'identification des menaces[G] génériques avec quantification de leur sévérité, suivie de l'identification des vulnérabilités[G] spécifiques liées aux types d'entités du SC et leur appréciation en termes de faisabilité ou de probabilité, le tout débouchant sur une liste de risques[G] spécifiques à prendre en considération;
- la confrontation des besoins de sécurité établis pour chaque fonction et catégorie d'informations (phase 1) aux risques[G] spécifiques (phase 3), mis en relation par le biais des entités[110].

Nous ne prétendons pas, loin s'en faut, avoir fait le tour d'EBIOS ni en maîtriser chaque élément, mais après cette première tentative de mise en oeuvre solitaire il nous semble qu'un certain nombre de questions méritent d'être relevées.

Lors de la sélection des éléments sensibles (première phase: étape 2, activité 1 (5.3.2)) nous avons été surpris de constater que EBIOS prenait uniquement en compte les fonctions et catégories d'informations essentielles. A aucun moment de cette activité, les entités exploitées par le SC et dont la liste figure au tableau 5.4 n'étaient prises en considération. Deux cas de figure, au minimum, peuvent cependant nous amener à considérer certaines entités comme critiques:

- *(8.4.a)* dans le cas d'un SC critique, les entités concernées deviennent automatiquement sensibles (il suffit d'imaginer par exemple l'impact sur un SC critique d'un problème de disponibilité[G] impliquant l'une de ces entités);
- *(8.4.b)* une entité (par exemple E_S_WAN) partagée par plusieurs applications (dont notre SC) peut être critique pour une de ces applications seulement (par exemple une activité ASP); le lecteur aura reconnu le problème à l'origine de notre réflexion sur l'écologie[G] des applications (4.6).

Si une entité devait être qualifiée de sensible pour un quelconque des domaines du SI (8.4.a), la valeur de cet attribut ne peut être ignorée au moment où l'on s'apprête à mettre cette même entité à contribution pour un autre domaine (une autre application) du SI *(8.4.c)*. Charge alors à l'étude de sécurité de décider des mesures à prendre: dédoubler l'entité sensible pour en éviter le partage, où établir des règles et scenarii précis régissant l'accès à l'entité. A notre sens, la démarche EBIOS gagnerait donc beaucoup à *permettre* (sans nécessairement *imposer*) la classification des entités en terme de sensibilité; l'idéal serait de permettre à une entreprise d'ajouter à EBIOS un dictionnaire reprenant toutes ses entités et leur niveau maximal de sensibilité. C'est dans ce dictionnaire que l'évaluateur d'un nouveau projet irait puiser les entités dont il aurait besoin pour mener à bien son étude (des objets, en somme), et pour chacune de ces entités, la valeur associée de sa sensibilité (un attribut).

[110] Puisque les fonctions et catégories d'informations utilisent des entités dont les vulnérabilités[G] spécifiques ont mené à la construction de la liste des risques[G] spécifiques.

Nous nous sommes par ailleurs trouvés confortés dans cette opinion par l'approche du CEA dont une des recommandations préconisait la classification de tous les objets en termes de disponibilité[G], intégrité[G] et confidentialité[G] [111]. Sans entrer dans des détails d'implémentation hors sujet, une technologie de classification sous forme de MIB comme cela se pratique au niveau du protocole SNMP paraît envisageable et pourrait constituer un pas vers une plus grande formalisation de la méthode.

Seconde curiosité de cette première phase, le fait que l'évaluation de la sensibilité des informations ne semble pas tenir compte de l'éventuelle découpe en sous-systèmes. Or, pour prendre un exemple, il nous semble a priori qu'une catégorie d'informations comme I_COMM serait beaucoup plus sensible au niveau du sous-système serveur (où transiteraient toutes les communications) que d'un sous-système distant *(8.4.d)*.

La deuxième phase nous a posé un autre problème, celui du type de relation à considérer pour établir les liens entre fonctions ou catégories d'informations et entités (tableau 5.5). La documentation n'est pas trop précise à ce sujet et parle au mieux de *liens existants entre les fonctions et les entités contribuant à leur réalisation d'une part, et entre les catégories d'informations et les entités contribuant à leur traitement* (5.2) (tableau 5.5). Cette définition peut parfois faire l'objet d'interprétations différentes, avec les conséquences finales que l'on imagine dans la mesure où une fois établis, ces liens sont à la base de la confrontation des risques[G] aux besoins à la phase 4.

La troisième phase a malheureusement vu ce genre d'imprécision atteindre des niveaux plus élevés. La liste des vulnérabilités[G] spécifiques (ANNEXE 8) manque singulièrement de clarté mais n'est pourtant accompagnée d'aucun élément explicatif: les termes *système*, *logiciel*, *réseau*, *programme*, *fichier-programme* ou encore *applicatif* sont utilisés fréquemment mais ne sont nulle part définis; le terme *matériels* semble parfois recouvrir les seuls éléments de hardware, et parfois englober le système d'exploitation; enfin, l'alternance d'expressions comme *facilité de*, *possibilité de*, *susceptibilité de* ou *fragilité de* sèment immanquablement le trouble dans l'esprit de quiconque essaye de conserver une cohérence d'ensemble à ses estimations de *faisabilité* et de *probabilité* (ANNEXE 9).

En plus de l'ambiguïté relative à certain des termes utilisés, un certain nombre de difficultés supplémentaires se sont manifestées principalement autour du sens qu'il fallait donner à la question que nous devions nous poser pour chaque vulnérabilité[G] [112]. Par exemple pour des vulnérabilités[G] comme *possibilité de créer ou modifier des commandes systèmes* ou *facilité d'accès à la commande de climatisation*, doit-on apprécier la faisabilité *intrinsèque*[113] de la chose ou estimer si cette vulnérabilité[G] spécifique est significative par rapport à la menace[G] générique tenant compte d'autres facteurs[114] ? Selon le contexte, répondre à cette question n'est pas toujours un exercice trivial.

D'autres questions, par exemple celles relatives à certaines menaces[G] logicielles (*infection par des virus, piégeage du logiciel*) sont tout simplement insolubles dans la mesure où, comme c'est le cas a priori pour le sous-système serveur, nous ignorons parfois encore tout à ce stade du *type du serveur* (architecture PC ou AS400 ?), de son *système d'exploitation* (Linux ou Windows ?), ainsi que des logiciels qui y seront exécutés (nature et origine). Pour contourner cet obstacle, deux alternatives nous semblent possibles:

- soit établir l'étude des risques[G] plus tard, une fois que certains options auront déjà été prises qui éviteront ce genre d'ambiguïté, mais alors les résultats de l'étude des risques[G] perdraient autant de chance d'influencer utilement ce processus de décision,
- soit faire en sorte qu'il soit possible, plutôt que de quantifier la vulnérabilité[G] d'un élément dont nous ignorons encore tout, de choisir ici une valeur de vulnérabilité[G] *maximale autorisée* pour ledit élément, mais alors nous ne sommes plus dans une étude des vulnérabilités[G] mais dans une spécification d'exigences.

La seconde possibilité, qui nous semble malgré tout la plus réaliste, n'est pas sans rappeler la notion de *seuil du tolérable* utilisée dans le chapitre précédent (7.1.5.b).

---

[111] ANNEXE 5, tableau A5.2, fiche de recommandation numéro 4: classification des objets.

[112] *Quelle est la probabilité ou la faisabilité que la vulnérabilité spécifique VS liée à l'entité E du SC permette à la menace générique MG de se réaliser* (8.2.3.a) ?

[113] La réponse serait, pour la climatisation: *oui, s'il est facile d'accéder à la commande de climatisation alors la probabilité de réalisation de la menace est grande.*

[114] La réponse serait, pour la climatisation: *non, parce que la commande de la climatisation n'est accessible que de l'intérieur de la salle des serveurs où seul le personnel autorisé et qualifié peut pénétrer.*

Pour en finir avec la phase 3, nous voudrions encore attirer l'attention du lecteur sur le fait que les valeurs de sévérité associées aux menaces[G] génériques (tableau 8.3 et ANNEXE 7), puis ventilées et réévaluées selon les risques[G] spécifiques (tableau 8.5 et ANNEXE 10), n'ont en fait jamais été exploitées par EBIOS - sinon sous une forme simplement binaire[115] à l'étape suivante. Nous nous sommes servis, de notre propre initiative, des valeurs de ces évaluations pour les combiner aux valeurs de faisabilité ou de probabilité liées aux risques[G] dans le but d'écrémer notre liste de risques[G] significatifs en ne conservant que les plus importants (8.2.4); mais lors de la confrontation des risques[G] aux besoins (8.2.5), c'est cette seule notion binaire d'existence ou de non existence de l'évaluation de la sévérité qui détermine pour chaque critère si le besoin réel de sécurité est égal à la sensibilité (existence de l'estimation) ou n'existe pas.

La conséquence immédiate de ce qui précède est que, pour une même fonction ou catégorie d'informations, nous obtenons un nombre différent de valeurs d'impacts réels (phase 4: tableau 8.6 et ANNEXE 12) suivant le sous-système considéré[116], mais lorsqu'elle existent les valeurs elles-mêmes de ces besoins sont identiques puisque, comme nous le faisions remarquer plus haut au sujet de la première phase, la sensibilité des informations ne tient pas compte de l'éventuelle découpe en sous-systèmes. Prenons un exemple pour éclaircir ceci: si nous comparons la menace[G] 38 du tableau 8.8 à la menace[G] 38 du tableau 8.9, nous voyons que dans le premier cas nous avions estimé qu'il y aurait un impact possible en disponibilité[G] et pas dans le second (ce qui correspond à la présence ou non d'une estimation de la sévérité de cette menace[G] pour ce critère dans le sous-système considéré[117]). Si par contre nous regardons les valeurs des impacts réels, nous constatons que là où elles existent dans les deux tableaux, elles sont obligatoirement identiques, ce qui nous paraît difficilement défendable. A notre sens, comme observé plus avant (8.4.d), nous devrions pouvoir établir des valeurs de sensibilités différentes selon le sous-système, ou sinon pouvoir les pondérer en fonction de l'évaluation de la sévérité des menaces[G].

Enfin, et pour terminer, nous dirions notre profond agacement devant les nombreuses petites variantes qui existent entre la manière de procéder telle qu'implémentée par le logiciel, celle qui est illustrée par le *case study* et celle que l'on trouve dans le guide [EB-G] ou la description des techniques [EB-T]. Plus d'une fois nous sommes restés perplexes devant une activité, et alors que nous pensions pouvoir trouver rapidement de l'aide via l'Internet et l'un ou l'autre groupe d'utilisateurs nous avons du nous rendre à l'évidence suivante : EBIOS ne semble connu qu'en France (et encore), et n'être utilisé tel quel que par des grandes entreprises publiques ou semi publiques (EDF, par exemple) *(8.4.e)*. Mais ces gens là ne tiennent pas de forums sur la question ; la plupart des autres sites que nous avons trouvés étaient des sites de sociétés de consultance en sécurité, qui disaient utiliser entre autres un outil *inspiré* de EBIOS, ou une version EBIOS *simplifiée*, ce qui mérite d'être signalé.

[115] Existence ou non existence d'une valeur de sévérité supérieure à zéro.

[116] Puisque la sévérité des menaces a été établie séparément pour chaque sous-système et que c'est l'existence d'une sévérité non nulle par rapport à un critère qui détermine que la valeur du besoin de sensibilité de la fonction ou catégorie d'information par rapport à ce même critère détermine la valeur de l'impact réel (8.2.5.a).

[117] Comme il y a normalement plus de monde dans E_L_SITE que dans un E_D_SITE, on peut imaginer que laisser un poste client avec un utilisateur authentifié sans personne à proximité ouvre davantage de possibilités.

Quatrième partie LA TECHNOLOGIE

Cette partie sera consacrée à l'évocation technologique de certains éléments évoquées dans les chapitres précédents, évocation destinée à compléter notre connaissance générale du domaine et - partant - à nous permettre de poser ultérieurement les bons choix.

Chapitre 9 Notions de base

Dans ce chapitre, nous rappelons les principales notions sans lesquelles la compréhension des chapitres suivants pourrait s'avérer ardue. Le lecteur familiarisé avec les concepts des réseaux est invité à passer directement au chapitre 10.

9.1. Introduction

9.1.1. Motivation

Il nous semble difficile de commencer à parler technologies et protocoles sans rappeler rapidement les concepts fondamentaux que nous allons utiliser. La plus grande partie de ce qui suit est extraite de [Tanenbaum-97] et de [INFO2231].

9.2. Les réseaux

9.2.1. Diversité

Un réseau peut être défini comme une *collection d'ordinateurs reliés entre eux*. Beaucoup de disparités existent au niveau du mode de connexion physique (type de câblage, sans fil hertzien ou pas, etc.), de la topologie (étoile, point à point, etc.), du mode de communication (broadcast[G], multicast[G], unicast[G], etc.) et des protocoles qui peuvent y être utilisés pour permettre tel mode de communication sur telle topologie en fonction du canal (medium) de connexion physique. Si nous définissons maintenant l'Internet (le théâtre de notre projet) comme étant le *réseau des réseaux* - c'est-à-dire une interconnexion de réseaux - nous avons une vague idée de la diversité des éléments constituant notre aire de jeux.

9.2.2. Modèles de référence

Pour permettre de concevoir efficacement des protocoles et des applications en réseaux, il s'est très vite avéré indispensable de masquer toutes ces disparités en utilisant un modèle en couches, chaque couche fournissant un certain nombre de services à la couche sus-jacente (quand il y en a une) et exploitant ceux qui lui sont offerts par la couche sous-jacente (quand il y en a une). L'incontournable modèle de référence de l'OSI, constitué de 7 couches, est illustré à la figure 9.1.

La couche *physique* s'occupe de la transmission des bits au travers d'un canal de communication (impulsions électriques et synchronisation). La couche *liaison de données*, au sein de laquelle ces bits sont organisés en trames, est chargée d'organiser la transmission de celles-ci d'un bout à l'autre d'une liaison, fournissant à la couche réseau un service de transmission qui lui paraisse exempte d'erreurs (l'organisation en trames permet à la couche liaison de données d'assurer la détection et la correction d'erreurs de transmission ainsi que le contrôle de flux). La couche *réseau* est chargée d'assurer le déplacement de datagrammes d'une source vers une destination, ce qui peut nécessiter de traverser de nombreux routeurs (et sous-réseaux) intermédiaires.

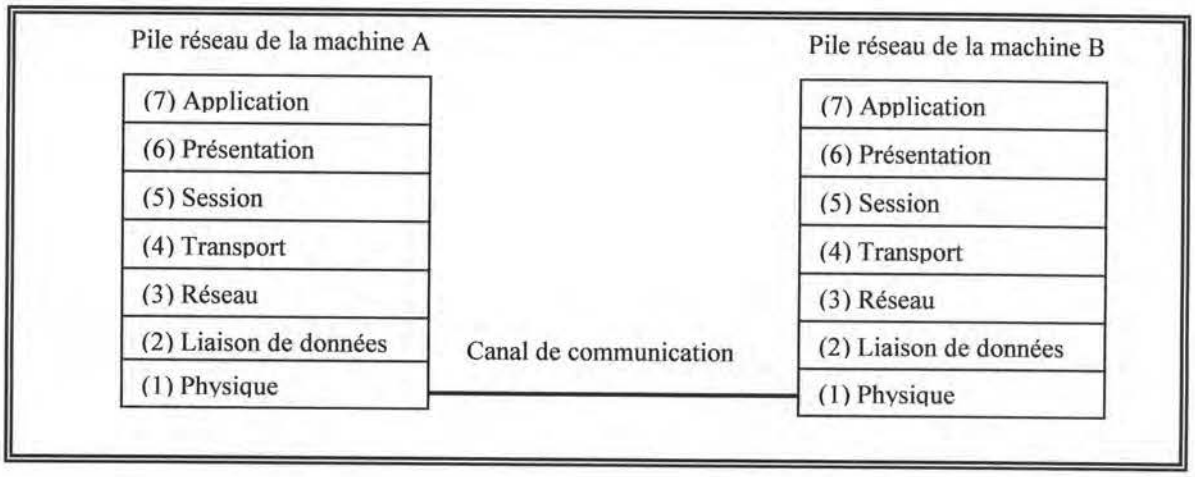


Figure 9.1: modèle de référence OSI

Les couches *session* et *présentation* ne nous intéressant que très modérément ici, nous dirons pour conclure cette survol du modèle de référence OSI que la couche *transport* est chargée de recevoir les données que lui fournissent les *applications*, de les découper le cas échéant en plus petites unités (paquets) et de les transmettre à la couche réseau tout en s'assurant éventuellement que tous les morceaux arrivent bien à destination de l'autre côté (isolant *de facto* les applications des évolutions éventuelles des couches sous-jacentes). Ce raccourci nous amène tout naturellement à la figure 9.2, laquelle représente le modèle de référence TCP/IP.

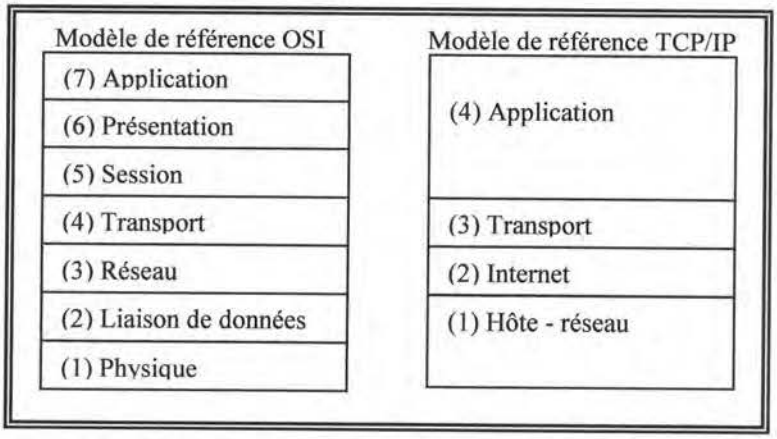


Figure 9.2: modèle de référence TCP/IP comparé au modèle de référence OSI

Ce modèle TCP/IP, du nom des protocoles les plus connus qui en font partie, est le modèle qui correspond à l'Internet tel que nous le connaissons aujourd'hui. C'est ce modèle que nous utiliserons par défaut.

9.3. Les protocoles

9.3.1. Les principaux protocoles de l'Internet

Le modèle de référence de TCP/IP est peu loquace au sujet de la couche hôte-réseau (OSI 1 + 2), se contentant d'exprimer *la nécessité que l'ordinateur puisse se connecter au réseau en utilisant des protocoles adéquats lui permettant d'envoyer et de recevoir des datagrammes IP.* Au sujet de ces protocoles (OSI 2, liaison de données), nous nous contenterons ici de rappeler les noms des plus connus qui sont PPP, HDLC ou encore FRAME RELAY. C'est aussi à ce niveau que se situent les protocoles d'exploitation des LAN comme par exemple l'Ethernet qui devait donner naissance à la norme IEEE 802.3.

Au niveau de la couche 2 dans l'Internet (OSI 3, réseau), le protocole IP est celui qui nous intéresse au premier chef. Juste au-dessus (OSI 4), la couche transport est représentée principalement par les protocoles TCP et UDP alors qu'au niveau de la couche 4 (application, OSI 5,6 et 7) nous trouvons les protocoles les plus connus du grand public parmi lesquels nous citerons HTTP, mais aussi FTP, DNS, NNTP et SMTP.

9.3.2. Le protocole IP

Le protocole IP[118] assure le routage des paquets reçus de la couche transport entre une source et une destination. Il s'agit d'un service non fiable[119] (perte de datagrammes possible, arrivée possible des datagrammes dans le désordre, etc.) et sans connexion (les datagrammes sont simplement émis). De plus, les datagrammes émis peuvent être fragmentés en cours de route selon les caractéristiques des couches hôte-réseau rencontrées.

Chaque datagramme IP contient un en-tête (minimum 20 octets) et une charge utile dont la taille peut atteindre 65535 octets moins la taille de l'en-tête. L'en-tête contient entre autres un champ *type de service* (codé sur un octet) qui permet en théorie aux routeurs de choisir la meilleure route pour le datagramme en fonction du type de service qui lui est associé et qui peut être:

- service avec délai de transmission minimum
- service avec débit de transmission maximum
- service avec fiabilité de transmission maximum

En pratique, ces informations sont relativement peu exploitées.

Signalons encore que le protocole IP permet plusieurs types de transmission: la transmission de type *unicast* [G] (un émetteur et un récepteur), la transmission de type *multicast*[G] (un émetteur et plusieurs récepteurs) et la transmission de type *broadcast*[G] (émission destinée à tous les hôtes d'un même réseau[120]).

9.3.3. Le protocole TCP

Le protocole de transport TCP (OSI niveau 4) utilise les services de la couche 2 (protocole IP) pour offrir aux applications de la couche 4 un transport fiable orienté connexion (l'établissement de la connexion entre l'émetteur et le récepteur est appelé le *handshake*).

Pour que le transport soit fiable alors qu'il s'appuie sur une couche Internet qui ne l'est pas, TCP doit gérer l'envoi et la réception d'accusés de réception, le réagencement des paquets (qui peuvent arriver dans le désordre), la détection des erreurs de transmission[121] et des pertes de paquets.

Lorsqu'un paquet est corrompu, est perdu ou si son accusé de réception n'est pas parvenu à l'émetteur avant l'expiration d'un temporisateur, celui-ci va le réémettre. Comme la perte d'un paquet peut aussi signifier une surcharge d'un routeur intermédiaire, l'émetteur utilise également un mécanisme qui consiste, quand une perte est détectée, à diminuer drastiquement son débit d'émission puis à l'augmenter progressivement selon un algorithme qui doit lui permettre de tendre vers la vitesse d'émission la plus proche du débit maximum que le réseau lui permet d'atteindre (*slow start*). Le récepteur, quant à lui, attend le paquet manquant pour pouvoir livrer à la couche application les données complètes, correctes et ordonnées.

Chaque paquet TCP contient un en-tête (minimum 20 octets) et une charge utile; la taille maximale du paquet correspond à la charge utile maximale d'un datagramme IP. Pour terminer, rappelons que TCP ne supporte que le mode de transmission *unicast*[G].

---

[118] Nous nous limitons ici à une description minimaliste du protocole IP version 4 (IPv4).

[119] Un total de contrôle, qui couvre l'en-tête du datagramme IP, permet de déceler certaines erreurs de transmission.

[120] C'est à dire tous les hôtes capables de communiquer entre eux sans traverser de router.

[121] Un total de contrôle couvre l'ensemble du paquet, en-tête et charge utile, et permet de déceler les erreurs de transmission.

9.3.4. Le protocole UDP

A côté de TCP, le protocole de transport UDP (OSI niveau 4) utilise les mêmes services de la couche 2 (protocole IP) pour offrir aux applications de la couche 4 un transport non fiable et sans connexion. Mis à part cela, UDP fonctionne de manière à peu près comparable à TCP mais comme il n'assure aucun contrôle de congestion ni aucune gestion de flux (même la somme de contrôle peut être désactivée), la taille de son en-tête a été ramenée à 8 octets.

UDP est utilisé là où il n'est pas nécessaire d'établir puis de libérer une connexion pour chaque couple de question/réponse, là où on peut se permettre de perdre quelques paquets de temps en temps sans que cela ne perturbe l'application outre mesure, ou encore quand le débit est plus crucial que la fiabilité.

Comme IP, UDP supporte les modes de transmission *unicast*[G], *multicast*[G] et *broadcast*[G].

9.3.5. Exemple de synthèse

Pour illustrer la dynamique des choses, prenons l'exemple d'une navigateur qui enverrait une requête à un serveur HTTP situé dans le même LAN: le contenu de la requête (une commande applicative comme *GET / HTTP 1.0*) est transmis par le navigateur (application) à TCP (transport), qui ajoute son en-tête puis transmet le(s) paquet(s) correspondant(s) à IP (internet), qui ajoute son en-tête puis transmet le datagramme au protocole de la couche hôte réseau (par exemple un protocole de la famille IEEE 802), qui encapsule le tout entre des *marqueurs* pour constituer une trame, laquelle est confiée au niveau physique (OSI niveau 1) pour être transmise comme un simple train de bits jusqu'à la machine de destination. Là, le même processus s'effectue en sens inverse et notre suite de bits redevient trame, dont le datagramme IP est extrait, lui-même libérant sa charge utile qui n'est autre que notre paquet TCP: après suppression de l'en-tête, TCP transmet la commande à l'application (un serveur HTTP). Ce principe d'encapsulations successives est illustré par la figure 9.3.

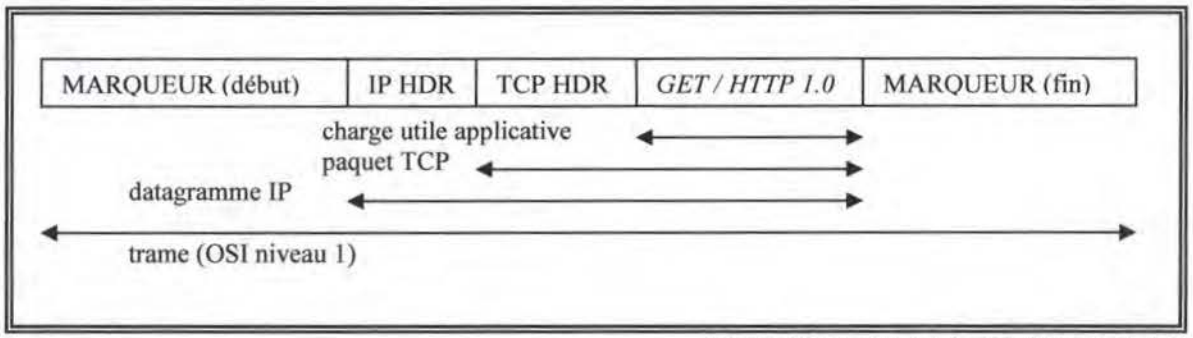


Figure 9.3: représentation de l'encapsulation

Cette illustration simple du principe d'encapsulation (conséquence du modèle en couches) nous permet de visualiser deux choses importantes: l'indépendance des protocoles entre eux pourvu que les services de chaque couche soient rendus et que leurs interfaces correspondent aux spécifications, et la surcharge que constituent les en-têtes successifs.

9.4. La voix

9.4.1. Caractéristiques

La voix humaine, comme tout type de son, est constituée d'une succession d'ondes acoustiques caractérisées par une fréquence f et une amplitude A. Pour transporter la voix sur un réseau IP, il est nécessaire de la numériser d'une manière efficace par rapport aux objectifs poursuivis. Or nos objectifs sont simples et faciles à énoncer: permettre des conversations de qualité téléphonique entre humains.

La numérisation de la voix sera donc considérée comme efficace si elle rencontre ces objectifs, c'est-à-dire si la voix numérisée (et elle seule) est audible et un minimum reconnaissable (pas question de haute fidélité).

Les seules fréquences sonores considérées seront donc celles qui constituent la tessiture de la voix humaine (approximativement entre 0 et 4000 Hertz), et ceci même si notre oreille nous permet en théorie de capter des sons allant jusque 22000 Hertz.

9.4.2. Digitilisation

La digitalisation de la voix consiste à échantillonner celle-ci à intervalles réguliers et à représenter chaque échantillon sous forme d'une suite de bits: les problèmes à résoudre sont donc ceux de la bonne fréquence d'échantillonnage et de la bonne représentation de ces échantillons.

La fréquence d'échantillonnage est dictée par le théorème de Nyquist, selon lequel tout signal sonore peut être digitalisé efficacement aux conditions suivantes:

- le signal choisi doit être échantillonné à une fréquence minimale de $2*f$
- le signal sonore doit être mesuré et représenté exactement

La première condition nous instruit que dans notre cas l'échantillonnage se fera à la fréquence 2*4000 Hertz minimum (ce qui correspond à un échantillon toutes les 125 microsecondes). La seconde condition est plus délicate, mais dans le cas de la téléphonie il s'avère qu'un échantillonnage sur 8 bits (soit sur base d'une échelle de valeurs comprises entre 0 et 255) est tout à fait acceptable.

Un rapide calcul nous permet donc de constater que la digitalisation de la voix humaine génère un trafic de[122] (charge utile uniquement, en-têtes pas comptabilisés):

8 bits / échantillon * 8000 échantillons / seconde = 64000 bits /seconde

9.4.3. Optimisations

Par rapport à ce qui précède, un certain nombre d'optimisations ont été qui tiennent compte des caractéristiques de l'oreille et des interactions humaines:

- en ne transmettant rien quand il n'y a rien à transmettre (suppression des silences)
- en utilisant des techniques de compression avec perte (notre oreille n'étant pas numérique, un certain lissage est autorisé);
- en ne transmettant pas les signaux de fréquence f' d'amplitude A' lorsque ces derniers sont plus ou moins émis simultanément par rapport à des signaux de fréquence f et d'amplitude A tels que f =+/- f' et $A >> A'$ (signaux masqués, inaudibles);
- en établissant des modèles de la voix, ce qui permet de ne transmettre que les paramètres de ces modèles;
- en transmettant des différentiels et non systématiquement des valeurs absolues.

L'utilisation combinée de plusieurs de ces mesures a permis de diminuer sensiblement la bande passante nécessaire de 64 kbps à 32 kbps[123], 16 kbps[124], 8 kbps[125] et même 6,3 kbps[126] (charge utile uniquement, en-têtes pas comptabilisés).

9.5. Typologie des applications

9.5.1. Les applications opportunistes ou élastiques

Certaines applications, dites *opportunistes* ou *élastiques*, vont tirer parti des ressources réseau disponibles[127] et si ces ressources diminuent, elles continueront à fonctionner (jusqu'à un certain point) mais simplement un

[122] Selon la norme G.711 (PCM) de l'ITU.
[123] Norme G.726 de l'ITU.
[124] Norme G.728 de l'ITU.
[125] Norme G.729 de l'ITU.
[126] Norme G.723.1 de l'ITU.
[127] Typiquement, la bande passante et les délais de transmission.

petit peu plus lentement. Ces applications peuvent être de type *interactif* (exemples: TELNET, transactions HTTP), de type *batch* (exemples: NNTP feed[128], FTP-data[129]) ou de type *requête-réponse* (exemples: NFS, requêtes DNS).

Les applications élastiques de type *interactif* ont typiquement besoin de fiabilité et de délais de transmission raisonnables; les applications élastiques de type *requête-réponse* ont surtout besoin de délais de transmissions courts, alors que les applications élastiques de type *batch* requièrent habituellement la fiabilité avant tout.

9.5.2. Les applications de type streaming

Les applications de type streaming, par contre, sont des applications dont on pourrait dire qu'elles fonctionnent à flux tendu: elles ont besoin d'un quota minimum de ressources et ne seront opérationnelles que si ce quota est disponible. D'autre part, si davantage de ressources réseau venaient à se libérer elles n'en tireraient pas nécessairement parti. Parmi les principales applications de ce type, citons les applications de type *multimedia conversationnel* (le cas de figure de notre application), les applications de type *multimédia interactif* (exemple: un jeu distribué) et les application de type *multimédia non interactif* (exemple: enseignement à distance).

Ici, les applications de type *interactif* requièrent principalement de courts délais de transmission, alors que le *multimedia non interactif* a davantage besoin de disposer d'une bande passante continue que de délais de transmissions extraordinaires. D'une manière générale, les applications de type multimédia peuvent très bien s'accomoder de quelques pertes d'informations.

9.5.3. Applications et choix de protocole

D'une manière générale, les applications qui ont besoin de fiabilité s'appuieront sur le protocole de transport TCP, alors que celles pour lesquelles la rapidité prime seront mieux servies par le protocole de transport UDP. UDP est également le seul des deux protocoles de transport à supporter le *multicast*[G].

9.6. Conclusions

Au lu de ce qui précède il apparaît clairement que la solution de transport idéale pour notre application de téléphonie via l'Internet est une solution UDP, et ce pour les raisons suivantes:

- la fiabilité des transmissions est relativement peu importante (quelques pertes d'échantillons ne rendent pas la conversation impossible);
- la rapidité des transmissions est importante: or, la *fiabilité* de TCP risque d'introduire des délais de transmission prohibitifs en cas de mauvaise qualité du réseau (pendant le temps d'attente pour l'expiration d'un temporisateur et le temps que le paquet réémis parvienne à destination, celle-ci ne transmet rien à l'application);
- le mécanisme de *slow start* par lequel, en cas de perte de paquets, TCP diminue son débit d'émission peut s'avérer incompatible avec une application de type streaming;
- la possibilité d'émettre en *multicast*[G] pourrait représenter un avantage (pour peu que ce mode soit supporté par les transporteurs).

Pour ces raisons, TCP est rarement utilisé pour transporter la voix. Toutefois, UDP a lui seul ne peut suffire parce qu'un certain nombre de mécanismes y font défaut: en effet, si la perte de quelques échantillons de temps en temps n'affecte pas la qualité globale de la conversation, il importe quand même pour éviter de trop grandes distorsions que les échantillons reçus soient livrés à l'application en séquence et au bon moment (n échantillons intermédiaires perdus doivent être remplacés par n éléments de remplissage de manière à ce que l'échantillon $n+1$ soit livré à l'application au temps correspondant). Or, nous avons vu que:

- *(9.6.a)* UDP ne réorganisait pas les informations reçues hors séquence;
- *(9.6.b)* UDP ne détectait pas les pertes;

[128] Transferts de gros volumes entre serveurs NNTP.

[129] Le protocole (application) FTP utilise deux connexions TCP: une connexion de contrôle (type interactif) et une connexion données (ftp-data: type batch).

- *(9.6.c)* UDP ne gérait pas les variations de délais.

Pour ces raisons, l'IETF a choisi de construire, au-dessus de UDP un autre protocole de transport (en fait, plutôt une sorte de librairie utilisable par les applications multimédias): le protocole RTP.

Chapitre 10 La voix sur IP

Présentation de quelques normes et protocoles relatifs au transport de la voix sur IP.

10.1 Introduction

10.1.1. Normes et organismes normalisateurs

Traditionnellement l'apanage des opérateurs téléphoniques, la voix se répand aujourd'hui progressivement sur l'Internet. Ce passage d'un monde dominé par les technologies de commutation de circuit vers le monde de la commutation de paquets s'accompagne du besoin de transposer vers l'Internet et son principal organisme normalisateur, l'IETF, une partie des normes éditées par l'ITU.

Au sens large, le transport de la voix s'effectue sur base d'une architecture logicielle à 3 couches, caractéristique du mode *streaming*, et qui comprend:

- le codage et le décodage de la voix (effectué par l'intermédiaire d'un algorithme spécialisé ou CODEC),
- la mise en paquets de la voix codée (ainsi que l'opération inverse d'extraction du paquet),
- la signalisation et le transport lui-même

10.1.2. Les normes ITU

L'ITU a établi plusieurs séries de normes dont celles qui nous intéressent ici sont:

- les normes audio, qui définissent les méthodes de codage et de décodage (CODEC); citons par exemple la norme G.711 (*pulse code modulation of voice frequencies*);
- les normes dites de transport[130], comme par exemple:
  - H.225: *call signalling protocols and media stream packetization for packet-based multimedia communication systems*
  - H245: *control protocol for multimedia communications* (échange et négociations des paramètres)
- les normes "cadre", qui regroupent et chapeautent les autres, et parmi lesquelles nous épinglerons H.323 qui correspond à l'adaptation aux réseaux à commutation de paquets des normes H.320 (ISDN) et H.324 (PSTN) régissant les communications téléphoniques.

Dans un environnement H.323, l'établissement de la communication est effectué au moyen du protocole Q.931 (H.225). Le protocole RAS (H.225) sert à l'enregistrement des équipements terminaux et au contrôle d'admission à la communication. H.245 permet de commander les applications de bout en bout, lesquelles se servent chacune d'un protocole spécifique (par exemple, T.120 pour les données).

10.1.3. Les normes IETF

L'IETF n'est pas directement concernée par le problème du codage / décodage audio et en conséquence les normes G711 et autres de l'ITU seront utilisées telles quelles dans le monde de l'Internet. La norme H.323 de l'ITU, en temps que norme "cadre", est également utilisée comme référence dans les deux univers mais le passage du monde des télécommunications à celui des réseaux IP a exigé la transposition des normes de signalisation et de transport conçues pour les circuits commutés (ITU) vers d'autres conçus pour les réseaux à commutation de paquet (IETF).

[130] Pourtant bien de la couche application (modèle TCP/IP).

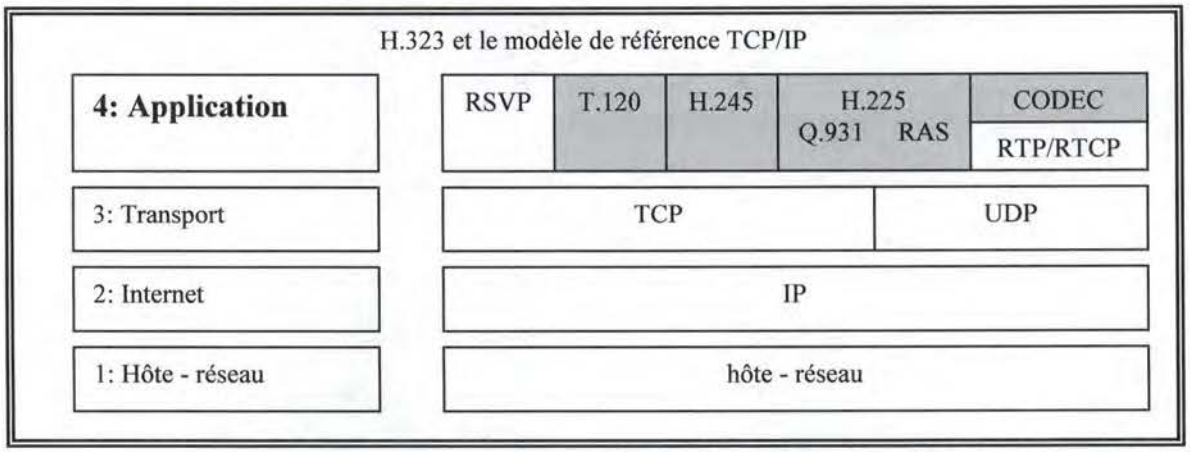


Figure 10.1: H.323 et le modèle de référence TCP/IP

La transposition au monde IP de H.225 et H.245, a donné naissance entre autres au protocole SIP. SIP n'est pas le seul protocole qui a été créé à cette fin[131], mais il semble qu'il soit sinon le plus représenté, du moins un de ceux destinés à subsister.

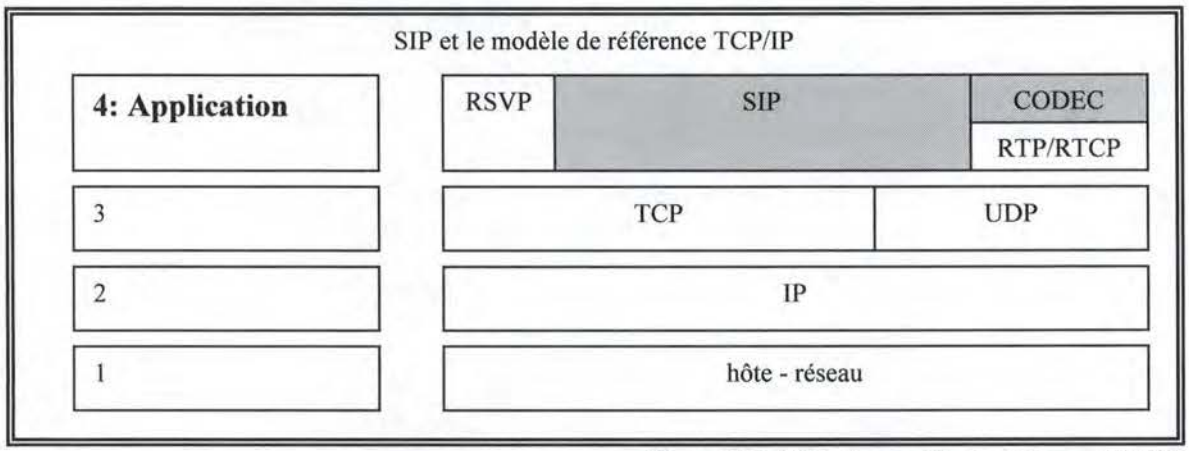


Figure 10.2: SIP et le modèle de référence TCP/IP

Un protocole de transport pour les applications de type multimédia via l'Internet a été décrit par [RFC1889], et les modalités spécifiques à l'audio l'ont été par [RFC1890]. Ce protocole, RTP, est donc un protocole générique permettant de transporter un nombre indéfini de flux multimédias (*payload types*), chaque type de flux faisant l'objet d'une description complémentaire. De plus, RTP est en fait constitué de 2 protocoles différents:

- le transport des flux multimédias s'appuie sur RTP;
- les mécanismes de contrôle des sessions[G] RTP (performances, retour d'information du récepteur vers l'émetteur) sont implémentés par RTCP.

D'emblée, signalons une certaine ambiguïté au niveau de la terminologie courante qui présente parfois implicitement RTP comme un protocole de transport (par exemple qund nous écrivons que *le transport s'appuie sur RTP*) alors qu'il s'agit bel et bien d'un protocole de la couche application.

[131] Citons aussi pour mémoire MGCP (en désuétude).

10.2. Session: protocole RTP

10.2.1. Objectifs

Les principaux objectifs poursuivis dans la cadre de la spécification du protocole RTP comprennent:

- *(10.2.1.a)* permettre le transport de la voix sur IP;
- *(10.2.1.b)* détecter les pertes et remplacer les paquets perdus par des 'blancs' [9.6.b] ;
- *(10.2.1.c)* détecter les inversions de séquence et réordonner les paquets reçus en désordre [9.6.a];
- *(10.2.1.d)* détecter les silences (suppression de blancs) et remplacer les paquets non émis par des 'blancs';
- *(10.2.1.e)* détecter les variations de délais de transmission et restituer chaque paquet à l'application exactement au moment voulu [9.6.c];
- *(10.2.1.f)* coder / décoder l'information en paquets.

Nous nous limiterons ici au cas des flux audio, alors que RTP permet de transférer aussi la vidéo.

10.2.2. Principe

Un émetteur (application) échantillonne et digitalise un signal audio puis le transmet à RTP après codage éventuel, lequel s'appuie su UDP pour le transport sur le réseau. A la réception, RTP réordonne les échantillons reçus, remplace ceux qui ne sont pas arrivés en temps utile par des 'blancs' puis les transmet au récepteur (application) dans la bonne séquence et en respectant strictement l'intervalle utilisé lors de l'échantillonnage. Ce principe est illustré par la figure 10.3:

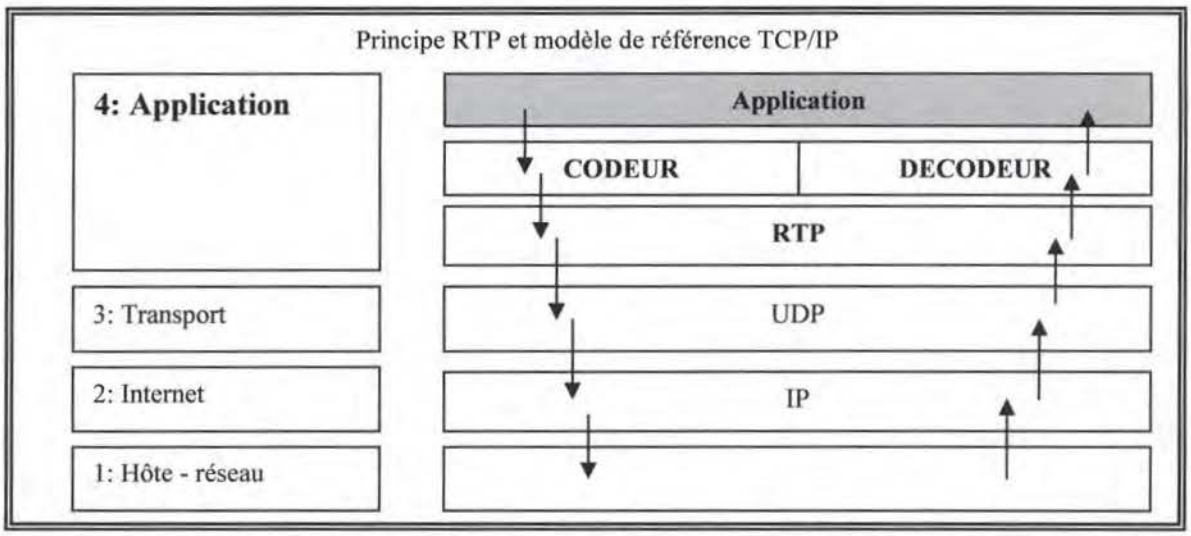


Figure 10.3: Principe RTP et modèle de référence TCP/IP

10.2.3. Le paquet RTP

Lorsque de la voix est transportée sur IP, la charge utile du datagramme IP est typiquement composée de trois parties:

- l'en-tête UDP (8 octects),
- l'en-tête RTP (12 octets) et
- la charge utile de RTP,

les deux dernières parties constituant la charge utile de UDP. Nous ne nous attarderons pas sur l'en-tête UDP qui ne constitue pas notre préoccupation du moment; au niveau du paquet RTP, nous trouvons les champs suivants (figure 10.4):

- V(2 bits): version du protocole;
- P (1 bit): indique si le payload contient du remplissage (padding) à la fin. Le dernier octet du payload indique le nombre de caractères de remplissage insérés.
- X (1 bit): indique si l'extension de l'en-tête est utilisée;
- CC (4 bits): indique combien d'adresses de contributing sources (CSRC) suivent l'en-tête fixe.
- M (1 bit): utilisé pour signaler la fin d'une période de suppression de silence;
- PType (7 bits): type d'encodage (de charge utile), par exemple tels que ceux définis dans [RFC1890];
- Numéro de séquence (incrémenté en continu): permet au receveur de détecter les pertes et les inversions de séquences;
- Timestamp (temps relatif auquel le paquet a été généré par l'application): permet au receveur de détecter l'absence de paquets (suppression de silences) et de savoir à quel moment il doit restituer le prochain paquet à l'application;
- SSRC identifier (32 bits): identification de la source qui a émis le paquet.
- champ d'extension de l'en-tête (optionnel)
- charge utile

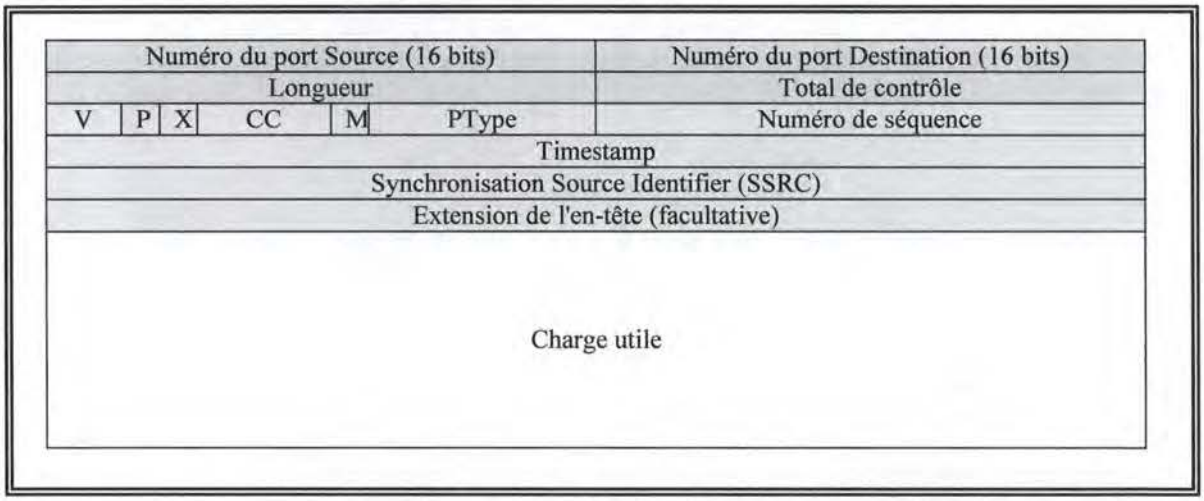


Figure 10.4: charge utile habituelle d'un datagramme IP transportant de la voix

10.2.4. Emission

Nous avons vu en 9.4.2 un exemple de codage selon la norme ITU G.711 dont le débit utile était de 64 kbps, ainsi que le taux de compression qui pouvait être atteint grâce à certaines optimisations comme par exemple ce que permet la norme ITU G.729 (compression 8:1, ce qui donne en moyenne, avec 8000 échantillons par seconde, un bit par échantillon).

Une fois ces échantillons codés, RTP leur ajoute son en-tête puis les transfère à UDP. Deux stratégies contradictoires sont possibles à ce stade:

- les transférer un par un au fur et à mesure qu'ils sont prêts, ce qui minimalise le délai à la source mais s'avère très pénalisant en terme de pourcentage d'overhead (header UDP + header IP);
- les regrouper à plusieurs dans un paquet UDP, ce qui diminue l'overhead mais augmente le délai à la source[132].

En effet, à raison de f échantillons par seconde, grouper n échantillons avant de les envoyer introduit d'emblée un délai de n/f secondes. Si par contre on décide d'envoyer un paquet UDP tous les b bits de données, le délai sera égal à $(b/c)/f$, avec c exprimant le nombre de bits par échantillon (après codage).Toute la difficulté consiste donc à choisir le bon équilibre entre la pénalisation liée à l'overhead (faible regroupement) ou celle liée au délai (fort regroupement).

[132] Par *délai à la source*, nous entendons la partie du délai de transmission imputable au seul émetteur, en faisant abstraction toutefois des délais proportionnellement bien plus faibles et par ailleurs relativement fixes qui sont imputables à la capture et au codage du son.

10.2.5. Réception

Du coté du récepteur, les échantillons reçus sont réagencés (sur base du numéro de séquence) et ceux qui se sont perdus (ou n'ont pas été émis) sont remplacés par des 'blancs' (sur base du timestamp)[133]; ensuite vient le moment de transmettre ces échantillons dans le bon ordre et au bon rythme vers l'application.

Toute la difficulté ici provient donc du fait que le transport s'appuyant sur une couche Internet (IP) non fiable, ces échantillons arrivent au récepteur après des délais de parcours variables, obligeant le RTP récepteur à les thésauriser quelques temps pour attendre certains des retardataires. Cette opération, qui consiste à introduire un délai de transmission à la destination, s'effectue à l'aide d'un *playback buffer*. En pratique, le délai de transmission introduit à la destination sera lui aussi variable, puisque l'objectif est que le délai de transmission total (fictif) soit fixe. Par exemple, si on accepte un délai de transmission total de 200 ms pour un réseau dans lequel le délai de transmission réel minimum serait de 50 ms, le playback buffer doit être à même de conserver à tout moment jusqu'à 150 ms d'échantillons; tout échantillon arrivant après un temps de parcours supérieur à 200 ms sera écarté, mais en attendant, la plus grande partie des erreurs de séquences et variations de délais sera corrigée.

Au plus grand le *playback buffer sera*, meilleure sera la qualité mais moins bonne l'interactivité, et inversement. Pour fixer les idées par un exemple concret, les communications téléphoniques par canal satellite souffrent de délais de transmission totaux avoisinant les 500 ms, et l'interactivité des conversations n'y est pas facile[134].

10.2.6. RTP et multicast

L'utilisation en mode *multicast*[G] pose 2 problèmes supplémentaires qui sont les différences entre les bandes passantes dont chacun dispose et le fait que le *multicast*[G] ne soit pas accessible partout.

Lorsque plusieurs receveurs disposent de bandes passantes différentes, plutôt que d'obliger tout le monde à travailler au débit de l'utilisateur le moins bien équipé, un relais RTP appelé *mixer* peut être inséré à proximité de la zone où se situe(nt) le(s) débit(s) inférieur(s). Ce mixer peut recevoir les différents paquets émis par les autres participants et reconstruire un flux plus lent à destination de la (ou des) station(s) réceptrice(s) lente(s). Dans ce cas, le mixer devient la nouvelle SSRC, mais l'identification de la (des) source(s) réelle(s) peut être maintenue en listant les *contributing sources* (CSRC) dans l'extension optionnelle de l'en-tête RTP[135].

Un autre type de relais RTP appelé *translator* transmet les paquets sans en modifier le SSRC. Les *translators* peuvent être des agents destinés à modifier le format de codage (sans mixer les flux), destinés à agir en tant que *application level filters* (proxy), ou destinés à convertir le trafic *IP multicast*[G] en *IP unicast*[G] et inversement. Deux *translators* de ce dernier type peuvent donc créer entre eux une sorte de tunnel *unicast*[G], permettant de traverser des portions de réseau dans lesquelles le mode *IP mulicast*[G] n'est pas supporté.

10.3. Contrôle: protocole RTCP

10.3.1. Objectifs

Les principaux objectifs poursuivis dans la cadre de la spécification du protocole RTCP visent à:

- permettre un retour d'information quant à la qualité de réception et au contrôle de congestion ;
- permettre d'identifier l'émetteur;
- permettre d'évaluer le nombre de participants en *multicast*[G];

[133] En réalité, certaines implémentations de RTP font mieux que cela en introduisant une forme de redondance grâce à laquelle un ou plusieurs échantillons perdus peuvent être partiellement récupérés sans réémission.

[134] Si nous considérons un satellite de communication sur une orbite géostationnaire à 35800 kilomètres de la terre, le seul temps de parcours aller et retour d'un faisceau hertzien entre un point sur l'équateur et un satellite à sa verticale (trajet minimum) sera d'approximativement (2 * 35800 km) / (300000 km/s), soit 239 ms.

[135] Ce qui permet au receveur d'indiquer à tout moment quelles sources ont contribué au son reproduit, fonctionnalité très appréciée quand tous les participants ne se connaissent pas bien.

10.3.2. Principe

De temps en temps, les entités communicantes s'échangent des rapports via RTCP. Les *sender reports*, envoyés par les émetteurs, permettent aux receveurs de connaître le volume d'information que chaque émetteur a envoyé depuis son précédent sender report[136]. Les *receiver reports*, envoyés par chaque receveur pour chaque source entendue, annoncent la qualité de l'information reçue de la source correspondante (identifiée par son SSRC)[137].

RTCP permet également l'échange d'informations d'identification de la source, ou SDES (Source DEScription). Les informations contenues, typiquement nom, adresse e-mail, téléphone, alias, etc., proviennent de l'application qui utilise RTP.

Enfin, les différents rapports échangés permettent à tout un chacun d'estimer le nombre de participants en mode *multicast*[G].

10.3.3. Le paquet RTCP

Le paquet RTCP est constitué d'un en-tête fixe comme celui du paquet RTP suivi d'une ou de plusieurs informations de contrôle identifiée(s) par leur type qui prendra une des valeurs suivantes:

- SR pour sender report;
- RR pour receiver report;
- SDES pour la description de la source;
- BYE pour indiquer que l'émetteur quitte la session[G];
- APP pour des informations spécifiques à un type d'application.

10.3.3. RTCP et multicast

Le fonctionnement en mode *multicast*[G] induit un certain nombre de contraintes supplémentaires, puisqu'avec la multiplication des senders et receivers il ne faudrait pas que le traffic RTCP finisse par saturer le traffic RTP. Au plus de participants donc, au moins de rapports chacun sera autorisé à envoyer. Ce qui signifie que si 5% des participants ne disposent pas d'une bonne connectivité, RTP risque bien de ne jamais s'adapter sauf si cette information remonte jusqu'à l'application et que cette dernière dispose de règles pour contraindre - éventuellement selon le profil des participants - RTP à en tenir compte.

Un certain nombre de mécanismes - paramétrables par l'application - permettent également à RTCP de se limiter à ne consommer qu'une fraction définie de la bande passante disponible pour le taffic RTP.

10.4. La signalisation: SIP

10.4.1. Objectifs

Les objectifs de la signalisation sont très orientés téléphonie et implémentent dans le monde de l'Internet l'interopérabilité des deux mondes et des différents types d'équipement existants (utilisation de combinés téléphoniques IP, passage de l'IP vers des infrastructures de type PABX et inversément, etc.). En deux mots, SIP a été conçu pour établir, modifier (ajouter ou supprimer des participants) ou terminer une session[G] multimédia, en mode unicast[G] ou multicast[G] (ou les deux), ce qui sous-entend:

- recherche et détermination du système terminal à joindre: rechercher un correspondant sur base d'une adresse e-mail, d'une adresse IP, etc. (via des protocoles comme DNS);

[136] Les *sender reports* contiennent en fait le volume total envoyé depuis le début de la session, mais à cette information sont associés l'heure en temps absolu (basée sur NTP) et la valeur correspondante de l'horloge interne à 8KHz utilisée, dans le cas de l'audio échantilloné à cette fréquence, pour le Timespamp de l'en-tête RTP.

[137] Les *receiver reports* mentionnent le dernier *sender report* reçu de la source en question, le temps écoulé depuis sa réception, le dernier paquet reçu, le nombre et la proportion des paquets non reçus et une estimation des variations des délais de transmission par rapport à cette source.

- détermination du mode d'accès à ce correspondant et des paramètres à utiliser: choix éventuel d'un gateway IP/PSTN pour joindre un correspondant via son numéro de téléphone, ou obtenir l'adresse IP d'un gateway H.425 puis faire appel à H.225 pour joindre un correspondant dont il a déterminé qu'il pouvait l'être via H.323, etc.
- détermination de l'état du correspondant (est-il apte à répondre à une invitation[G], etc.);
- détermination des capacités du correspondant (types de médias, et paramètres associés, que ce dernier accepte);
- contrôle des autorisations d'accès au réseau de chacun des interlocuteurs;
- initialisation de la session[G] (démarrage de RTP avec les paramètres négociés), transfert de la session[G], terminaison la session[G].

Pour mémoire signalons encore qu'en plus de RTP, SIP peut coopérer avec des protocoles comme RSVP pour réserver des ressources réseau, ou encore SAP (annonce des sessions[G]) et SDP (description des sessions[G]).

10.4.2. Principe

SIP est un protocole de la couche applications (modèle de référence TCP/IP), indépendant des protocoles réseau et de transport sous-jacents, qui définit un certain nombre de services fonctionnant fréquemment sur base du principe de brèves associations requête-réponse (appelées *transactions* SIP). SIP implémente les fonctionnalités suivantes:

- l'adressage: chaque correspondant (ou groupe de correspondant) éventuel est identifié par un URI unique (exemple: *sip:sales@my.company.com*[138]);
- la localisation, qui permet de déterminer où et comment joindre un correspondant;
- la redirection, ou réponse apportée à une demande de localisation effectuée directement par un client SIP auprès du service de localisation;
- la fonction de serveur proxy SIP, qui transmet en son nom propre toutes les demandes (y compris de localisation) reçue d'un client[139];
- l'enregistrement, qui permet à un client SIP d'informer un serveur proxy ou un serveur de redirection de l'endroit où on peut le joindre[140];
- l'implémentation des méthodes du protocole, comme par exemple l'invitation[G] (méthode 'INVITE'). C'est via ces différentes primitives que la négociation des paramètres a lieu.

10.4.3. Sécurité

Les spécifications de SIP indiquent que les proxy SIP peuvent demander aux clients qui les contactent de s'authentifier et, lorsque c'est le cas, ces proxy SIP sont fermement invités à vérifier si la requête introduite est autorisée pour le client authentifié. La méthode d'authentification[G] prévue est celle définie par [RFC2617] pour HTTP, et consiste simplement à permettre au serveur de demander au client de lui fournir un nom d'utilisateur et le mot de passe correspondant, informations transmises soit en texte clair (mode 'basic') soit sous forme d'un digest MD5 (mode 'digest') généré sur base d'une chaîne aléatoire reçue du serveur. La manière dont les noms d'utilisateurs et mots de passe sont initialement communiqués au serveur n'est pas définie, et la sécurité réelle qu'offrent ces méthodes d'authentification[G] est considérée comme relativement faible [RFC3261].

Des mécanismes visant à garantir l'intégrité[G] et la confidentialité[G] des messages SIP existent également et sont fondés sur S/MIME. Nous n'entrerons pas ici dans le détail de tels mécanismes, mais nous contenterons d'en dire qu'ils sont mis en oeuvre lors de l'échange de paramètres divers précédent l'établissement d'une session[G] RTP.

---

[138] La syntaxe de l'URI est beaucoup plus développée et variée que cet exemple le ferait croire, puisqu'elle peut comprendre aussi bien un véritable numéro de téléphonie classique que des informations sur les paramètres acceptés par l'utilisateur.

[139] Quand un serveur proxy SIP reçoit une réponse à une demande de localisation, celle-ci n'est pas retournée au client: le proxy contacte directement le serveur qui lui aura été renseigné.

[140] Il peut pour ce faire utiliser l'adresse multicast "all SIP servers" (sip.mcast.net ou 224.0.1.75).

10.4.4. Conclusions

Nous ne nous étendrons pas davantage sur l'aspect signalisation sinon pour constater que dans le contexte contrôlé de notre projet, où les utilisateurs ne peuvent être en mesure d'établir eux-mêmes leur répertoire, la plupart des fonctionnalités avancées de recherche de l'interlocuteur et de communication via l'Internet ne nous sont d'aucune utilité et représentent même un risque[G] important de détournement du système (menace[G] EBIOS numéro 31, *utilisation illicite du matériel,* avec impacts possibles en disponibilité[G]). Qui plus est, nous ne sommes pas opérateurs réseaux et, partant, notre système de téléphonie sera de nature opportuniste[141] (pas de réservation de ressources via RSVP). En d'autres termes, il existe relativement peu de recouvrement entre les objectifs d'un tel système de signalisation (10.4.1) et les besoins propres de notre application; toute la difficulté consistera à déterminer si ce recouvrement suffira à justifier l'utilisation d'un protocole comme SIP ou s'il peut être plus judicieux de s'en passer.

10.5. Essai d'application

10.5.1 Objectif

Nous avons voulu effectuer une petite évaluation de la faisabilité de l'utilisation de RTP vis-à-vis d'un de nos plus gros clients. La question que nous nous sommes posés est donc de savoir si le niveau actuel des performances du réseau permettait ou non l'utilisation de RTP entre ce client et nous. Pour ce faire, nous sommes partis des hypothèses suivantes:

- les valeurs de RTT mesurées entre le router du client (chez lui) et son serveur d'application localisé au siège central de l'entreprise sont représentatives de la réalité;
- ces valeurs de RTT peuvent être assimilées à un délai de transmission entre la station de travail d'un employé et le router du client, transmission dont le chemin passerait par le siège central de l'entreprise.

10.5.2. Echantillonnage

Le matériel de base pour cette évaluation est constitué d'une série de 47610 valeurs de RTT prises en continu à raison d'environ une valeur toutes les 10 secondes entre le 13 mai 2003 au matin et le 28 mai 2003, milieu de journée[142]. Ces valeurs sont le résultat d'autant de ICMP ECHO ('ping') empruntant la connexion VPN établie entre le router du client et celui de l'entreprise, ce qui implique que:

- à quelques rares exceptions près (fermeture du VPN), aucun ICMP n'a été perdu (le VPN implémente une encapsulation TCP), mais en contrepartie le RTT a pu être surévalué en cas de *retry*;
- le délai tient compte du temps de chiffrement et de déchiffrement (clé symétrique de 128 bits), ce qui contribue à surévaluer le RTT;
- la bande passante du VPN, strictement limitée, est exploitée en priorité par le client pour accéder à ses applications en mode ASP et est découpée en trois files d'attente de trafic[143]:
  - le trafic RDP, prioritaire: file d'attente 0;
  - le trafic LPD, non prioritaire: file d'attente 2;
  - le reste du trafic (DNS, SMTP, ICMP, ...): fille d'attente 1;

Tous ces éléments contribuent probablement à une surévaluation des valeurs de RTT que nous aurions si nous avions réalisé ce test hors VPN.

---

[141] Ce qui ne signifie pas que, comme les applications qualifiées d'opportunistes (9.5.1), il pourra fonctionner plus ou moins bien selon la disponibilité des ressources du réseau. Simplement, quand ces ressources ne seront pas suffisantes, il ne fonctionnera pas et nous nous rabattrons alors sur des outils plus traditionnels (4.3.2.a).

[142] La série n'est pas totalement complète, dans la mesure ou les *backup routers* qui sont régulièrement mis en service pour vérification n'avaient pas été configurés pour procéder à cet échantillonnage. D'autre part, seules les mesures prises entre 7h et 18h ont été prises en considération..

[143] La politique d'allocation de l'accès au canal est simple: une file d'attente n (avec n > 1) est autorisée à accéder au canal si et seulement si la file d'attente n-1 est vide.

10.5.3. Le délai end to end

Le délai total ou délai *end to end* (de bouche à oreille) d'une transmission RTP est constitué de la somme des délais suivants:

- le délai à la source:
  - délai de capture du son (pour mémoire)
  - délai de quantification[144] (pour mémoire)
  - délai de compression: au plus performant l'algorithme, au plus grand le délai de compression;
  - délai de paquetisation: au plus d'échantillons on regroupe, au plus grand le délai de paquetisation;
  - délai éventuel de chiffrement (pour mémoire)
- le délai de transmission
  - délai d'accès au canal
  - délai de transmission réseau
- le délai à la réception:
  - délai éventuel de déchiffrement (pour mémoire)
  - délai fictif introduit par le *playback buffer*;
  - délai de décompression (même ordre de grandeur que le délai de compression)
  - délai de déquantification (pour mémoire)
  - délai de restitution (pour mémoire)

Les délais de quantification / déquantification sont cités pour mémoire seulement. Des valeurs indicatives pour les délais de compression figurent au tableau 10.1, tableau trouvé dans [INFO2231] et repris de [Tobagi-98][145]. Enfin, les délais de paquetisation et ceux liés au mécanisme du playback buffer ont été respectivement introduits en 10.3.4 et 10.3.5.

Tableau 10.1	**Délais de compression [Tobagi-98]**	
Norme	*Bande passante requise*	*Délai de compression*
G.711	64 kbps	0,75 ms
G.726	32 kbps	1 ms
G.728	16 kbps	3-5 ms
G.729	8 kbps	10 ms
G.723	6,3 kbps	30 ms

Au vu de ce qui précède, nous pouvons déduire que les délais que nous avons mesurés représentent les seuls délais de transmission et de chiffrement / déchiffrement.

10.5.4. Analyse des échantillons

La liste des RTT mesurés a été éditée en un fichier contenant une valeur par ligne, fichier ensuite traité à l'aide d'un petit programme C sans prétention repris en ANNEXE 14. Ce programme ventile les échantillons par classe (la partie entière du RTT), liste ces classes et leur contenu et établi un percentile qui nous apprend que sur cette période de 14 jours, 90% des ICMP REQUEST ont provoqué le retour d'un ICMP ECHO dans un délai de 93 ms, le délai minimum observé étant de 27 ms.

10.5.5. Optimisation des paramètres RTP

La difficulté réside ici dans la variabilité des situations rencontrées. La quasi-totalité des futurs utilisateurs de notre application disposent actuellement ou disposeront bientôt d'une connexion ADSL dont le débit en upload n'est quand même pas extraordinaire, ce qui devrait nous inciter à grouper davantage d'échantillons par unité de transport[146]. Si nous visons par exemple:

[144] Digitalisation.
[145] Cette dernière référence est citée mais n'a pas été consultée.
[146] Une valeur de 20 ms de signal audio par unité de transport est habituelle. Augmenter cette valeur diminue l'overhead mais augmente l'impact en cas de perte d'une unité de transport.

- un délai end to end de 200 ms (ce qui est acceptable sans être extraordinaire)
- un taux de compression moyen de 4:1[147] (qui nous paraît un bon compromis)
- le regroupement de 50 ms de signal audio par unité de transport (soit 50 ms / 0,125 ms/éch. = 400 échantillons audio par paquet UDP/RTP)

nous pouvons estimer notre taux de pertes probable comme suit:

Délai total end to end acceptable (fixe):	200 ms
Délai de capture et de quantification:	pour mémoire
Délais de compression:	005 ms
Délais de paquetisation:	050 ms
Délai de décompression:	005 ms
Délai de déquantification et restitution:	pour mémoire
Solde: délai disponible pour chiffrement, déchiffrement et transmission:	140 ms
Soit, d'après nos mesures, un percentile de:	93% à 94% (6 à 7% de pertes)

et nos besoins en bande passante:

Charge utile (bits):	(400 éch. * 8 bits/éch.) / 4 = 800 bits
Taille du datagramme IP:	320 bits + 800 bits = 1120 bits
Bande passante requise:	1120 bits/datag. * 8000 éch/sec : 400 éch/datag = 22400 bps[148]

Selon ce cas de figure et avec un taux de compression moyen, en plaçant 50 ms d'audio dans chaque paquet UDP, l'ensemble constituerait un stream que supporteraient même les connexions analogiques (modems 56 kbps). Evidemment, chaque échantillon perdu ou hors délai (6 à 7% du total) coûterait 50 ms d'audio, mais le taux de pertes pourrait diminuer dès lors que le trafic RTP serait extrait du VPN dans lequel nous avons effectué nos mesures et où il subit une féroce concurrence[149].

A titre de comparaison, si nous disposions d'un réseau optimal (ni perte ni congestion) et souhaitions utiliser TCP, nous aurions un des deux cas de figure suivants:

- soit TCP remplace UDP: la taille cumulée des en-têtes passerait de 320 à 416 bits et la bande passante requise passerait de 22400 bps à 24320 bps (augmentation de 8,6 %);
- soit UDP est encapsulé dans TCP: la taille cumulée des en-têtes passerait de 320 à 480 bits et la bande passante requise passerait de 22400 bps à 25600 bps (augmentation de 14,3 %);

Rappelons pour terminer que tout ceci n'est qu'un cas de figure concernant un seul client géographiquement assez proche. Pour d'autres clients, plus éloignés ou disposant d'une moins bonne connectivité, nous pourrions être confrontés à des RTT moins favorables; il importe dans ce cas que l'application adapte ou permette d'adapter en conséquence ces paramètres RTP.

10.6. Sécurité de RTP/RTCP

10.6.1. Mécanismes disponibles

Les informations dont nous souhaitons pouvoir garantir la confidentialité[G] correspondent au type *données non persistantes* que nous avions introduit en (4.4.1), à savoir le contenu des conversations (4.4.1.f), véhiculé par RTP, et l'identité des participants à une conversation (4.4.1.g), ce qui nous ramène au besoin de confidentialité[G] des *protocoles de l'application* (4.4.1.h) puisque ces informations sont véhiculées par RTCP (type SDES).

[147] Norme G.728 de l'ITU.
[148] Hors overhead lié au fonctionnement de la couche hôte-réseau (couche 1 du modèle de référence TCP/IP).
[149] Le trafic interactif (protocole *Remote Desktop Protocol* de Microsoft) y dispose d'une priorité absolue.

RTP et RTCP permettent le chiffrement en un bloc de tous les octets destinés à être encapsulés ensemble dans un même datagramme de transport[150]. En cas de chiffrement, un nombre aléatoire de 32 bits est inséré juste après l'en-tête des paquets RTCP pour déjouer les tentatives de décryptage sur base du texte connu. RTP ne requiert pas cette prévention puisque ses champs numéro de séquence et timestamp sont initialisés avec des valeurs aléatoires. Par défaut, l'algorithme de chiffrement utilisé est le DES en mode CBC, choisi pour sa facilité de mise en oeuvre et sa large distribution. D'autres algorithmes peuvent être choisis dynamiquement pour une session[G] mais ils devront être négociés via des moyens externes à RTP/RTCP, de même d'ailleurs que toute clé utilisée.

Toutefois, les concepteurs de RTP considèrent eux-mêmes cette possibilité interne de chiffrement comme un pis-aller destiné à n'être utilisé que lorsque les niveaux sous-jacents (comme IP) ne peuvent pas offrir ce service. Une autre possibilité, par eux avancée, consisterait à définir un nouveau type de *payload* qui serait par exemple *audio-chiffré* - charge à l'application de s'en occuper.

Le souci de préserver la disponibilité[G] transparaît uniquement dans le contexte où il est question de brider les échanges RTCP à une valeur ou une portion du trafic déterminée

Pour l'imputabilité[G] et l'intégrité[G], le besoin qu'ont ces critères de s'appuyer sur des ressources externes rend difficile leur implémentation au sein de RTP/RTCP; les concepteurs de ces protocoles estiment donc que la responsabilité de ces garanties incombe aux divers protocoles sous-jacents. L'authentification[G] (garante de l'imputabilité[G]) dans RTP est implicite et liée à la connaissance de la clé du chiffrement. Enfin, le seul outil de vérification de l'intégrité[G] est constitué par un certain nombre de *sanity checks* relativement triviaux, puisqu'ils consistent en quelques contrôles de cohérence au niveau de (ou sur base de) l'en-tête[151].

En conclusion, nous pouvons dire que RTP prévoit des mécanismes pour garantir la confidentialité[G] (chiffrement DES) ainsi que quelques algorithmes visant à empêcher RTCP de porter atteinte à la disponibilité[G] du protocole, algorithmes utiles surtout en environnement *multicast*[G]. Pour le reste, ou pour de meilleures garanties, RTP s'en remet à d'autres protocoles.

10.6.2. Limites

DES est ancien et le niveau de performances des processeurs actuels permet de casser ce genre de chiffrement assez aisément. Reste la possibilité ouverte d'utiliser un autre algorithme, à condition de disposer des protocoles ad-hocs pour en négocier la clé. Un autre problème que pose le chiffrement est que pour pouvoir faire leur office, chacun des *mixers* et des *translators* doit être à même de chiffrer et de déchiffrer la charge utile des paquets UDP, donc de connaître la clé de chiffrement pour cette session[G] RTP. Or, la dissémination de la clé de chiffrement rend celle-ci d'autant plus vulnérable. Et pour terminer avec le chiffrement, la définition d'un nouveau type de *payload* comme *audio-chiffré* ne garanti pas a priori la confidentialité[G] des informations de type SDES véhiculées par RTCP.

En ce qui concerne l'authentification[G] implicite, il faut signaler qu'elle ne permet pas d'authentifier un participant par rapport à un autre en mode *multicast*[G]. Si des moyens externes à RTP/RTCP ne sont pas mis en oeuvre pour authentifier chaque stream, rien n'empêche un participant d'émettre des paquets RTP et RTCP en utilisant le SSRC d'un autre (usurpation d'identité avec impact en disponibilité[G] pour la victime[152]). D'autres possibilités existent pour porter atteinte à la disponibilité[G], comme par exemple la simple émission d'un paquet RTCP contenant BYE en utilisant le SSRC d'un autre participant. Et qui plus est, si le chiffrement n'est pas utilisé, ces possibilités s'étendent également aux non participants[153].

---

[150] En cas d'envoi simultanés de plusieurs types de RTCP, par exemple SDES et RR, RTCP peut les séparer en deux paquets différents afin de ne chiffrer que le premier, le contenu du second (RR) étant d'un intérêt général pour les opérations de transport (opérateurs réseaux).

[151] Par exemple pour RTP: vérifier que la version du protocole soit bien égale à 2, que le type de *payload* soit connu, qu'il y ait bien un compteur dans le dernier octet si le bit 'P' est à 1, etc. [RFC1889]

[152] Le protocole prévoit que si un doublon est détecté au niveau du SSRC, les participants concernés doivent en changer; émettre de manière répétée en utilisant le SSRC d'un autre participant constitue donc également une attaque efficace de type *DoS*[G] (atteinte à la disponibilité).

[153] L'identification des participants se basant sur le SSRC et non sur l'adresse IP, il est très difficile - surtout en mode sans connexion - de différencier un datagramme IP légitime d'un datagramme IP dont l'adresse source aurait été modifiée.

Dernier écueil majeur à éviter: il ne faudrait pas non plus que le chiffrement devienne trop pénalisant en termes de temps de réponse. Par rapport aux délais de codage / décodage et de transmission, le chiffrement par DES-CBC ne devrait toutefois pas représenter une surcharge significative, mais nous avons vu qu'il n'offrait pas de garanties suffisantes.

10.8. Conclusions

Au terme de ce chapitre nous pouvons affirmer qu'à de nombreux égards le protocole RTP correspond exactement à nos attentes et ce pour les principales raisons suivantes:

- *(10.8.a)* il a été conçu pour ce genre d'application,
- *(10.8.b)* il est paramétrable, ouvert et
- *(10.8.c)* il peut s'adapter aux conditions de trafic.

Toutefois, certaines caractéristiques ou faiblesses du protocole ne peuvent être ignorées:

- *(10.8.d)* RTP ne gère que le transport: il est donc nécessaire de lui adjoindre un protocole de signalisation, mais des protocoles comme SIP nous paraissent particulièrement lourds par rapport à nos besoins;
- *(10.8.e)* RTP présente quelques faiblesses au niveau de la sécurité: clairement, authentification[G] et chiffrement sont à chercher ailleurs.

Utilisé seul, RTP doit impérativement exploiter ses possibilités de chiffrement. Mais un niveau de sécurité suffisant ne pourra être obtenu qu'en s'appuyant sur d'autres protocoles qui permettent d'assurer une authentification[G] et un chiffrement efficaces. Ces domaines de l'identification[G], de l'authentification[G] et du chiffrement font l'objet des chapitres suivants.

Chapitre 11 Identification et authentification

Dans ce chapitre nous passons rapidement en revue quatre approches de la problématique de l'identification[G] et de l'authentification[G], en vue de déterminer celle(s) qui correspondrai(en)t le mieux à nos besoins.

11.1. Introduction

11.1.1. Motivation

Le principe de l'identification[G] et de l'authentification[G] ayant été retenu (4.5.3.f) et les faiblesses en la matière d'un protocole comme RTP établies (10.8.e), il nous a semblé utile de passer en revue quelques-unes des principales méthodes d'identification[G] et d'authentification[G] existantes afin de déterminer quelle(s) formule(s) correspondrai(en)t le mieux à nos besoins sur base des critères retenus dans les chapitres qui précèdent. Ceci ne constitue donc pas une analyse exhaustive et comparative des protocoles et de leurs implémentations, mais une simple évaluation du type de solution qui serait de nature à nous satisfaire.

Pour simplifier et ramener le débat au cadre de référence de ce document, nous nous restreindrons dans ce chapitre à envisager l'identification[G] et l'authentification[G] d'un utilisateur humain (auquel nous associons tout processus agissant pour son compte et sous son contrôle) auprès d'un serveur (notre SC) via un réseau IP non sécurisé. Nous avons donc choisi de passer rapidement en revue dans ce chapitre quelques techniques d'identification[G] et d'authentification[G] simples qui auront été sélectionnées sur base des critères suivants:

- *(11.1.1.a)* ces techniques devront appartenir à des catégories différentes (en termes de technologie, de principe de fonctionnement ou d'algorithme mis en œuvre) et être suffisamment représentatives de leur catégorie;
- *(11.1.1.b)* elles ne devront pas nécessiter l'intervention d'un tiers (tiers de confiance)[154];
- *(11.1.1.c)* elles ne devront pas nécessiter l'utilisation d'un matériel périphérique spécifique (1.2.3.b).

Sur base de ces critères, nous avons choisi de passer en revue dans ce chapitre les techniques ou protocoles suivants:

- PAP (parce que PAP est *la* méthode historique),
- CHAP (pour la technique du *challenge*),
- S/KEY (pour son coté atypique) et
- une méthode d'authentification[G] biométrique.

11.1.2. Principe

L'identification[G] et l'authentification[G] regroupent des techniques permettant à un processus de s'assurer de l'identité d'un utilisateur[G], l'ensemble de cette procédure correspondant souvent au modèle simplifié suivant:

- l'utilisateur[G] décline son identité (identification[G]) au processus;
- l'utilisateur[G] prouve qu'il est bien qui il prétend être (authentification[G]);
- le processus accepte (réussite de la procédure) ou rejette (échec de la procédure) l'utilisateur[G].

[154] Cette option relativement arbitraire est motivée tant par le souci de maintenir ce document à des proportions admissibles (en introduisant un certain nombre de simplifications) que par l'absence de moyens réels alloués au projet (1.2.3.b) (le recours aux tiers de confiance et l'utilisation de certificats à des fins professionnelles étant rarement sans coûts).

La technique la plus fréquemment utilisée pour l'identification[G] consiste probablement à faire en sorte que le serveur vérifie l'existence et l'unicité de l'identité déclinée par l'utilisateur dans une liste d'utilisateurs habilités. L'authentification[G], quant à elle, se base sur un des trois piliers suivants:

- la connaissance: vérifier que l'utilisateur connaisse un secret partagé uniquement entre lui et le processus auprès duquel il souhaite s'authentifier;
- la propriété: vérifier que l'utilisateur soit en possession d'un objet bien personnel: une carte à puce, par exemple;
- l'état de l'utilisateur, par le recours aux techniques biométriques.

Pour être acceptée par nous, une telle procédure d'identification[G] et d'authentification[G] devra au minimum présenter les caractéristiques suivantes:

- l'impossibilité du rejeu: une séquence d'identification[G] et d'authentification[G] ne pourra être rejouée avec succès par une entité tierce qui l'aurait captée;
- la non compromission de l'utilisateur, en garantissant la confidentialité[G] des informations sensibles (le secret partagé, par exemple, ne peut être divulgué);
- la persistance: une fois la procédure effectuée avec succès, il ne doit pas être possible d'usurper l'identité de l'utilisateur authentifié (attaque du style *man in the middle*[G])[155].

11.1.3. Méthode

Dans les lignes qui vont suivre et pour nous aligner sur la terminologie rencontrée, nous utiliserons le terme de *secret* pour désigner la chaîne de caractères que l'utilisateur devra à chaque fois introduire (4.7.3.d) pour s'authentifier, et nous parlerons de *mot de passe* pour désigner la chaîne de caractères transmise au serveur en vue de l'authentification[G]. Il est important de signaler que l'utilisation du vocable *mot de passe* ne signifie pas que le protocole en question se limite à une authentification[G] par la connaissance (4.5.3.b), puisqu'aussi bien un élément matériel (carte à puce, ...) (4.5.3.c) pourrait intervenir dans la conversion du secret en mot de passe.

Pour chacun des 4 protocoles que nous avons choisis (11.1.1) nous procéderons comme suit:

- nous commencerons par une brève description du protocole, suivie de
- la mise en évidence de ses principaux avantages (forces) et inconvénients (faiblesses);
- nous décrirons ensuite quelques vulnérabilités[G] possibles et
- proposerons des solutions de nature à les atténuer, voire les faire disparaître.

11.2. PAP

11.2.1. Principe

PAP ou *Password Authentication Protocol* [RFC1334] est un protocole d'identification très simple, basé sur l'existence d'un *secret partagé* et conçu initialement pour l'identification au travers d'un lien point à point; à ce titre, PAP est implémenté par des protocoles comme PPP. Par facilité, nous parlerons de client (qui souhaite être identifié et authentifié) et de serveur (qui valide l'identification[G] et l'authentification[G]).

Une fois la liaison de données établie (OSI niveau 2) le client transmet (éventuellement à plusieurs reprises) au serveur et en clair son identité et un secret partagé (toujours le même, donc dit *réutilisable*); quand il se trouve en possession de ces deux éléments, le serveur répond par une notification de succès (l'identité lui est connue et le secret qui lui est associé est bien celui qu'il a reçu) ou d'échec (l'identité lui et inconnue ou le secret qui lui est associé ne correspond pas à celui qu'il a reçu) de l'identification.

[155] Comme nous ne traitons dans ce chapitre que des phases d'identification et d'authentification de l'utilisateur, nous ne considérons pas pour le moment les possibilités d'authentification de chaque paquet.

11.2.2. Evaluation

PAP est un protocole encore fort répandu et comportant plusieurs variantes qui partagent toutes l'avantage d'être d'une très grande simplicité d'implémentation et d'utilisation. Mais la plupart du temps ces variantes partagent toutes aussi un certain nombre de problèmes parmi lesquels les principaux nous paraissent être:

- le secret doit être connu des deux parties (risque[G] en confidentialité[G] au niveau de l'enrôlement[G] et des informations conservées sur le serveur);
- l'identité du client est transmise, et n'est habituellement pas chiffrée (4.5.3.g) ;
- le secret du client est transmis, et n'est habituellement pas chiffré (4.5.3.g);
- la cadence à laquelle les demandes d'identification peuvent être envoyées permet une attaque répétée de type 'dictionnaire' (par essais et erreurs);
- il n'y a pas de protection contre le rejeu (4.5.3.h);

Les protocoles PAP peuvent donc donner satisfaction dans les cas de connexion locale (terminal), ou de connexion à distance via ligne point à point dédicacée ou réseau sécurisé. Mais même dans ce contexte, le risque[G] d'avoir un intrus à l'écoute sur la ligne ne peut être négligé. Par rapport à notre projet, ce genre de protocole ne satisfait évidemment pas nos exigences.

11.2.3. Améliorations possibles

Tenter d'améliorer PAP représente peu d'intérêt vu la disponibilité[G] d'autres protocoles, comme CHAP, qui ont été décrits à cette fin.

11.3. CHAP

11.3.1. Principe

Le protocole CHAP ou *CHallenge Authentication Protocol* [RFC1334] [RFC1994] est un protocole d'identification[G] et d'authentification[G] en trois étapes, basé sur l'existence d'un *secret partagé* qui n'est jamais transmis sur le medium de communication. Comme PAP (11.2), il est habituellement implémenté dans le cadre de liens point à point. Par facilité, nous parlerons ici aussi de client (qui souhaite être identifié et authentifié) et de serveur (qui valide l'identification[G] et l'authentification[G]).

Le serveur envoie au client qui a manifesté le souhait d'ouvrir une session un message contenant un *challenge*, suite de caractères choisie de manière aléatoire et idéalement unique (c'est à dire qui n'a pas déjà été utilisée) *(11.3.1.a)*. Le client utilise ce *challenge* pour générer un *mot de passe* (en utilisant un algorithme de hachage non réversible, comme MD5) à partir d'une chaîne de caractères contenant son *secret* et envoie ce *mot de passe* en réponse au serveur. Le serveur calcule lui-même le *mot de passe* sur base des mêmes

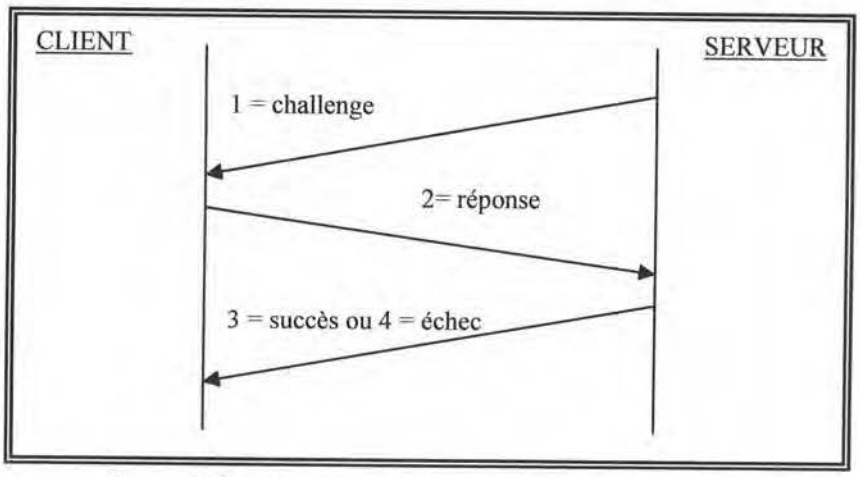


Figure 11.1: messages échangés lors d'une session CHAP

éléments et compare le résultat obtenu à celui reçu du client, puis lui communique le résultat de l'identification (succès ou échec).

Les messages de type 1 (challenge) et 2 (réponse) de la figure 11.1 ont un format commun qui est décrit au tableau 11.1.

La réponse (contenu du champ Valeur dans le message de Code = 2) est calculée par le client et le server en appliquant l'algorithme de hachage non réversible à la chaîne de caractères obtenue en concaténant dans l'ordre la valeur du champ *identifiant*, le secret, et la valeur du *challenge* (champ *valeur* dans le message de Code = 1). Les modalités pratiques (type d'algorithme de hachage à utiliser, etc.) auront été décidées au préalable par exemple via la négociation du protocole LCP qui établit la liaison de données pour PPP.

Dans les messages de type 3 et 4, les trois derniers champs sont remplacés par un champ 'Message' optionnel (texte).

Tableau 11.1	**Format des messages CHAP de types 1 et 2**	
Champ	*Longueur*	*Contenu*
Code	1 octet	Le numéro du message (voir la figure 11.1)
Identifiant	1 octet	*(11.3.1.b)* Utilisé pour identifier une session CHAP telle que décrite sur la figure 11.1.
LongueurT	2 octets	Longueur totale du message
LongueurV	1 octet	Longueur du champ Valeur qui suit
Valeur	0 à n octets	Challenge (Code = 1) ou réponse (Code = 2)
Nom	1 à n octets	Nom du serveur (Code = 1) ou du client (Code = 2) pour identification

11.3.2. Evaluation

CHAP représente une évolution majeure par rapport au PAP, et comporte un certain nombre de points forts:

- le secret (mot de passe) n'est pas transmis sur le lien (4.5.3.g); ce qui est transmis est un *one time password* (*OTP* ou mot de passe à usage unique, non réutilisable);
- il n'y a pas de rejeu (4.5.3.h) possible d'une séquence d'identification (11.3.1.a) (11.3.1.b);
- l'identification[G] et l'authentification[G] mutuelles sont optionnelles mais bien prévues par le protocole;
- *(11.3.2.a)* les séquences d'identification[G] et d'authentification[G] peuvent être répétées à plusieurs reprises au cours d'une connexion client - serveur (4.5.3.i), ce qui devrait permettre de bloquer les attaques du style *man in the middle*[G];
- il n'y a pas d'attaque directe possible par essais et erreurs.

L'explication de ce dernier point est simple: le protocole stipule que si plusieurs messages de type 2 (contenant le *mot de passe*) arrivent pour un même challenge (code *identifiant* (11.3.1.b)), seul le premier reçu doit être évalué et la réponse donnée à tous les autres (succès ou échec) doit être identique à celle donnée au premier. Une deuxième tentative implique donc un autre *identifiant* (11.3.1.b) et un autre *challenge*, donc un autre mot de passe.

Quelques faiblesses valent toutefois d'être signalées:

- le secret doit être connu des deux parties (risque[G] en confidentialité[G] au niveau de l'enrôlement[G] et des informations conservées sur le serveur);
- *(11.3.2.b)* le secret doit être conservé en clair sur le serveur (risque[G] en confidentialité[G]);
- l'identification[G] du client est transmise (4.4.3.d) en clair (4.5.3.g) dans la réponse (message de type 2: champ *nom*);
- *(11.3.2.c)* l'*identifiant* et le *challenge* étant transmis en clair, le secret n'est en théorie pas à l'abri d'une attaque indirecte de type 'dictionnaire' (notons toutefois la difficulté d'une telle attaque, la fonction de hachage étant du style 'n to 1');

- le protocole autorise mais n'impose pas la répétition périodique des séquences d'identification[G] et d'authentification[G] en cours de la connexion[G] (11.3.2.a).

En outre, si l'identification[G] et l'authentification[G] de type CHAP semblent donner satisfaction dans l'environnement point à point dans lequel il fut initialement implémenté il n'en va pas de même une fois qu'on le place dans un réseau public interconnecté contenant des intrus. Sa vulnérabilité[G] dans ce cas semble non seulement avoir été établie par modélisation du protocole [Leduc-99], mais aussi en pratique [Krahmer-02].

[Leduc-99] a démontré qu'un intrus pouvait tirer parti de la possibilité d'identification[G] et d'authentification[G] mutuelles si le secret partagé est le même dans les deux sens (ce qui était toutefois déjà fortement déconseillé par [RFC1994]). Le *challenge* envoyé par le serveur au client est intercepté par l'intru qui le renvoie tel quel au serveur, se faisant passer pour le client, puis utilise le *mot de passe* que lui renvoie le serveur (message de type 2) comme réponse au *challenge* initialement reçu de ce dernier *(11.3.2.d)*.

[Krahmer-02] constate de son coté que si le serveur n'est pas tenu de vérifier à nouveau l'identité du client au cours d'une connexion[G] (11.3.2.a), le client est quant à lui tenu de répondre à ce genre de requête. Dans un contexte d'un lien PPTP déjà établi entre deux machines d'un même LAN, Krahmer a montré qu'il était possible de générer un faux nouveau *challenge* auquel le client s'empresse de répondre correctement (succès), réponse captée et rejouée avec un égal succès par l'intrus (attaque du style *man in the middle*[G]) *(11.3.2.e)*.

Troisième cas de figure, présenté d'une manière légèrement simplifiée: si un protocole du type CHAP devait être exploité pour permettre à un client dans un LAN d'entreprise de s'identifier auprès d'un serveur distant, un intrus situé sur sa route (routeur compromis) pourrait aisément remplacer l'adresse IP du client par la sienne (SNAT ou Source NATting) et inversément au retour (DNAT ou Destination NATting) puis cesser de faire suivre les réponses du serveur vers le client une fois l'identification réussie. La connexion[G] serait alors ouverte entre l'intrus et le serveur, au moins aussi longtemps que ce dernier ne relance pas une nouvelle session CHAP *(11.3.2.f)*.

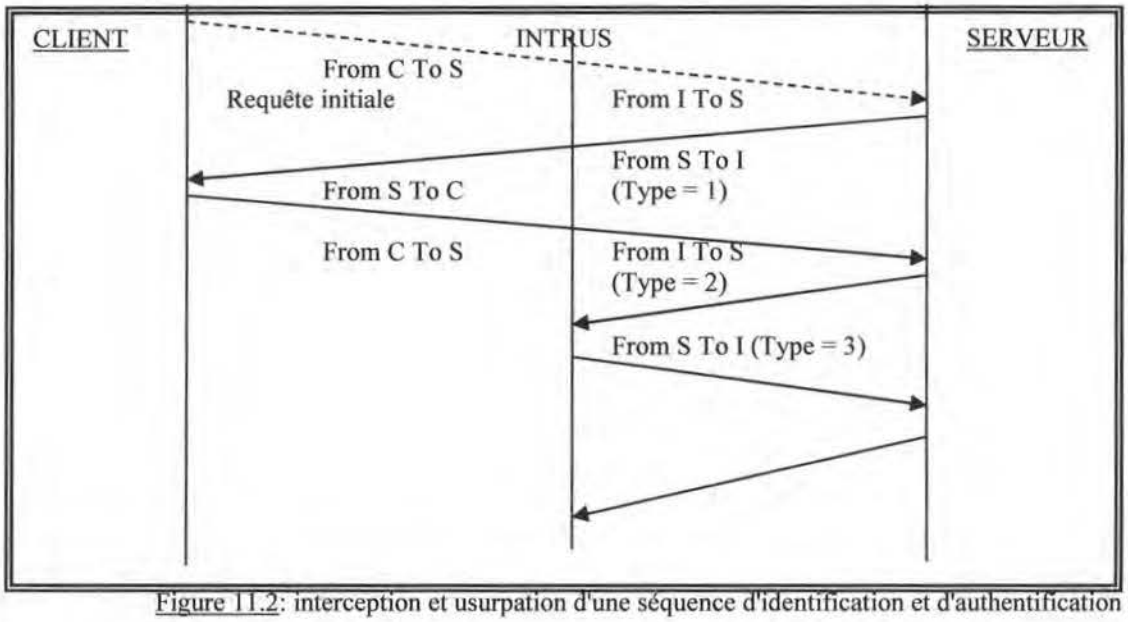


Figure 11.2: interception et usurpation d'une séquence d'identification et d'authentification

11.3.3. Améliorations possibles

Par rapport au premier cas de figure [leduc-99], une bonne mesure consisterait à imposer l'authentification[G] mutuelle avec des secrets différents *(11.3.3.a)*. Cependant, le prix à payer est double, puisque non seulement cela nous imposerait de conserver une donnée persistante (un secret pour le serveur) sur chaque client (4.4.3.c), et qui plus est de l'y conserver en clair (11.3.2.b). Une autre possibilité serait de limiter à une le nombre de sessions d'identification concurrentes *(11.3.3.b)*, interdisant alors au serveur de répondre à son propre *challenge* que lui aura retourné le faux client (11.3.2.d).

Pour les deux exemples suivants (11.3.2.e) (11.3.2.f), il nous semble devoir imposer la réitération aléatoire des sessions CHAP (11.3.2.a) *(11.3.3.c)*, ce qui par ailleurs n'est pas forcément pour nous déplaire (4.5.3.i). Il convient

toutefois de s'assurer au préalable qu'aucun client non identifié ni authentifié ne réponde à un *challenge* non sollicité par une requête initiale de sa part (voir figure plus haut) (11.3.2.e) *(11.3.3.d)*.

Une autre possibilité par rapport au dernier cas (11.3.2.f) consisterait à sceller le contenu des champs non variables du header IP, en transmettant avec chaque datagramme un hachage ou un CRC calculé sur une chaîne composée en concaténant les valeurs de ces champs avec celle du secret (garantissant l'intégrité[G] de l'IP source). Ce genre de solution, utilisé par exemple par le protocole AH sous IPSec, présente toutefois deux inconvénients: il augmente l'overhead des datagrammes et le temps de traitement (parfois gênant pour une application de type multimédia conversationnel) et elle n'est envisageable qu'à partir des dispositifs de protection logique de l'entreprise (plus précisément, de la machine assurant le SNAT ou Source NATting). En d'autres termes, cela ne nous protègera pas d'un intrus situé dans nos murs. Il conviendrait également de s'assurer, dans ce cas, que l'utilisation répétée du secret ne puisse pas représenter un facteur de risque supplémentaire (11.3.2.c).

Enfin, et d'une manière générale, il conviendrait autant que faire se peut d'éviter tout envoi d'information sensible (identité, challenge) en clair *(11.3.3.e)*.

11.4. S/KEY

11.4.1. Principe

Cette méthode d'authentification[G] décrite par [RFC1760] [RFC1938] met en oeuvre les éléments suivants:

- un *secret non partagé* (connu du seul client): s;
- un chaîne de caractères choisie aléatoirement à l'initialisation, constante par la suite, et conservée par le serveur: c;
- une fonction de hachage à sens unique H (initialement MD4);
- deux éléments de vérification, connus du serveur:
  - le résultat de n applications récursives de la fonction de hachage H au secret s concaténé avec la chaîne c, résultat que nous noterons $H^n(s+c)$;
  - la valeur correspondante de n.

L'authentification[G] du client par le serveur s'opère de la manière suivante:

- le client décline son identité [Haller-94];
- *(11.4.1.a)* sur base de l'identité déclinée, le serveur envoie au client l'identification de l'algorithme H utilisé, la valeur courante de n et la chaîne c (l'ensemble formant le *challenge*)
- le client communique au serveur le résultat de l'opération $H^{(n-1)}(s+c)$. Le serveur considère que l'authentification[G] est réussie si $H(H^{(n-1)}(s+c)) = H^n(s+c)$, auquel cas il remplace localement $H^n(s+c)$ par la nouvelle valeur $H^{(n-1)}(s+c)$ reçue du client, et décrémente n de 1.

S/Key étant en fait une marque déposée par les laboratoires Bell, plusieurs implémentations existent sous d'autres noms (OPIE, ...) et permettent d'utiliser d'autres fonctions de hachage (MD5, sha1).

11.4.2. Evaluation

Les avantages de cette manière de fonctionner sont intéressants, et nous citerons par exemple les 4 éléments suivants:

- le secret lui-même n'est pas conservé sur le serveur: seuls $H^n(s+c)$, c et la valeur initiale de n doivent être établis et communiqués (enrôlement[G])
- pas de rejeu possible (*one-time password*)
- grâce à la chaîne c, le même secret peut être utilisé pour plusieurs serveurs
- *(11.4.2.a)* en modifiant uniquement la valeur de la chaîne c quand $n = 1$, le système peut être réinitialisé (nouvel enrôlement[G] partiel pour $H^n(s+c)$) sans obliger l'utilisateur à changer de secret.

Au registre des inconvénients, signalons simplement

- *(11.4.2.b)* c, n et $H^n(s+c)$ étant transmis en clair, une attaque indirecte de type dictionnaire (11.3.2.c) reste théoriquement possible;
- *(11.4.2.c)* la nécessité de réinitialiser le système (11.4.2.a) toutes les *((valeur initiale de n) - 1)* identifications réussies impose de synchroniser avec le serveur des nouvelles valeurs pour au moins c et $H^n(s+c)$;
- *(11.4.2.d)* l'identité du client est probablement transmise en clair ([RFC1760] et [RFC1938] n'en font pas état).

Certaines vulnérabilités[G] ont toutefois été établies. A partir d'un router compromis, il serait aisé de se faire passer pour le serveur et sur base des informations préalablement recueillies (transmissions en clair (11.4.2.b) (11.4.2.d)) d'envoyer au client un challenge (11.4.1.a) comportant une valeur n_i bien inférieure à la valeur n_j qu'aurait envoyée le véritable serveur. Le client répondra en nous fournissant $H^{n_i}(s+c)$ que nous pourrons alors utiliser pour répondre avec succès à tous les *challenge* du serveur destinés au client abusé et comportant des valeurs de n telles que $n_i \leq n \leq n_j$ *(11.4.2.e)*.

On ne sait pas trop bien non plus comment les différentes implémentations du protocole se comporteraient si elles étaient confrontées à une situation de course: deux demandes de connexion[G] quasi simultanées (une émanant d'une client légitime et l'autre d'un attaquant) pourraient se voir proposer le même challenge, auquel la même réponse pourrait permettre aux deux demandes d'être satisfaites *(11.4.2.f)*.

Enfin, l'authentification[G] étant effectuée une seule fois, la faisabilité d'une attaque de type *man in the midde* ne peut pas être considérée comme nulle *(11.4.2.g)*.

11.4.3. Améliorations possibles

Nous pourrions encore proposer au protocole les quelques améliorations suivantes:

- *(11.4.3.a)* éviter tout envoi d'information sensible (identité, challenge) en clair (11.4.2.e);
- *(11.4.3.b)* conserver coté client la dernière valeur de n utilisée (pour chaque serveur) (11.4.2.e);
- *(11.4.3.c)* limiter à une le nombre de sessions d'identification concurrentes (11.4.2.f);
- *(11.4.3.d)* répéter les sessions d'identification ou chiffrer les échanges en utilisant une clé non dévoilée (11.4.2.g).

11.5. L'authentification biométrique

11.5.1. Principe

Pour définir le contexte dans lequel nous envisagerions d'introduire une méthode d'authentification[G] biométrique, rappelons les quelques contraintes suivantes:

- il n'y a pas de moyens financiers disponibles: il est donc difficile d'envisager l'achat d'un périphérique externe pour chaque poste client. Par ailleurs cette éventualité a déjà été écartée d'emblée au niveau de nos critères de sélection des protocoles (11.1.1.c);
- il est tout aussi difficile (contre-productif) d'imposer un tel achat au client;
- l'utilisation d'un périphérique externe imposerait pratiquement la fidélisation de l'utilisateur à son poste de travail privilégié (on imagine mal l'utilisateur transporter et connecter son périphérique externe là où il se trouve - en plus du micro)

C'est la raison pour laquelle nous envisageons l'étude d'une méthode d'authentification[G] biométrique par la reconnaissance de la frappe au clavier. Concrètement, une phrase choisie est tapée par l'utilisateur et un système enregistre la signature de la frappe (succession de durées: intervalle de temps entre chaque paire de lettres et durée de pression sur la touche pour chaque lettre): il s'agit de l'enrôlement[G]. A l'authentification[G], l'utilisateur introduit la même phrase, le SC en calcule la signature biométrique et l'authentification[G] est réussie si cette nouvelle signature correspond (à une *distance limite* près) à celle enregistrée lors de l'enrôlement[G].

Une discussion de cette méthode et un prototype ont été réalisés par [Philippe-02]; le lecteur intéressé trouvera les fondements théoriques[156] sur lesquels se basera notre évaluation ainsi que davantage d'explications sur le sujet en ANNEXE 15. Par rapport à ce que reprend l'ANNEXE 15, ajoutons que [Philippe-02] définit le *seuil de décision* comme la *distance relative*[157] à laquelle le *taux de fausse acceptation* (signature indûment acceptée) et le *taux de faux rejets* (signature indûment rejetée) sont égaux l'un à l'autre, et constate sur base de sa population test qu'à une distance relative de 34% les deux taux (TFA et TFR) se rejoignent en se situant entre 3,4 % et 3,9%. [Philippe-02] a donc choisi cette valeur de distance relative comme *seuil de décision* et considère qu'une signature pourra être acceptée si sa distance relative par rapport à l'échantillon de référence[158] est inférieure à la valeur de son seuil de décision.

11.5.2. Evaluation

Parmi les facteurs susceptibles d'influencer l'efficacité du système et avancés par [Philippe-02], nous avons voulu essayer d'en évaluer deux:

- *(11.5.2.a)* un facteur individuel: le niveau de fatigue (partant de l'idée que le niveau de fatigue est lié à l'avancement de l'heure dans la journée);
- *(11.5.2.b)* un facteur matériel: le type de clavier.

A ces deux facteurs nous ajoutons:

- *(11.5.2.c)* un facteur temporel: la dérive dans le temps.

Pour cerner ces différents facteurs, nous avons utilisé le prototype de [Philippe-02] pour nous enrôler et avons procédé par la suite à 155 authentifications[G] sur une période de quatre mois (11.5.2.c), authentifications[G] aimablement suggérées par le *scheduler* de notre station de travail 3 fois par jour à heures fixes (10h30, 16h30 et 22h30) (11.5.2.a).

Les mêmes informations d'enrôlement[G] ont ensuite été copiées sur une autre machine, dont le clavier était sensiblement plus dur; nous avons alors procédé à 3 séries de 30 authentifications[G] simultanées (15 par série et par machine) pour mesurer l'effet éventuel de la sensibilité du clavier [159] (11.5.2.c).

11.5.2.1. Validation de l'enrôlement

Notre première étape consistait à vérifier la qualité de l'enrôlement[G]. [Philippe-02] constatait que dans la majorité des cas, la distance relative entre chaque enrôlement[G] et les moyennes des enrôlements[G] était de l'ordre de 10 à 30%, alors que pour certains il dépassait 40% *(11.5.2.1.a)*. Avec une distance relative avoisinant les 16%, tant par rapport à la moyenne qu'à la moyenne sans extrêmes, nous considérons que la qualité de notre enrôlement[G] est satisfaisante.

Par la suite, vu la faible différence entre les deux types de moyennes, nous ne prendrons plus que la première en considération.

11.5.2.2. Influence du niveau de fatigue

Afin d'évaluer ce facteur, nous avons réparti nos 155 échantillons en trois classes (selon l'heure de leur saisie) et calculé pour chacune la moyenne des distances relatives. Les résultats de ces calculs montrent une tendance à l'augmentation de la distance relative en fonction de l'avancement de l'heure dans la journée, mais les différences restent peu significatives (tableau 11.2, page suivante)

Par contre ce que ce tableau ne montre pas mais que nous avons constaté, c'est l'augmentation très sensible du nombre de fautes de frappe en fonction de l'avancement de l'heure dans la journée.

---

[156] Les expressions comme *distance relative* utilisées dans ce chapitre y sont définies.

[157] Pour simplifier, disons que la *distance relative* est un pourcentage qui quantifie l'écart mesuré entre la signature à valider et la moyenne des 10 signatures générées lors de l'enrôlement[G] (échantillon de référence).

[158] Constitué d'une moyenne calculée sur base des 10 signatures générées à l'enrôlement[G].

[159] Les deux machines sont côte à côte dans le même environnement physique.

Tableau 11.2	**Evolution de la distance relative en fonction de l'heure**
Heure	*Moyenne des distances relatives*
10H30	17,90
16H30	18,29
22H30	18,90

11.5.2.3. Influence du type de clavier

Considérant que des variations du niveau de la sensibilité des claviers étaient plus fréquemment rencontrées que des variations au niveau du type de clavier (azerty/querty), nous nous sommes donc contentés de comparer une population de 45 authentification[G] effectuées via un clavier sensible avec une population équivalente d'authentifications[G] réalisées presque simultanément via un clavier plus dur.

Tableau 11.3	**Influence du type de clavier**							
Clavier	*Longueurs totales*		*Distances totales*		*Distances moyennes*		*Distances relatives*	
	Moyenne	*Dév. Std*	*Moyenne*	*Dév. Std*	*Moyenne*	*Dév. Std*	*Moyenne*	*Dév. Std*
Sensible	2138,64	143,02	510,14	60,73	34,01	4,05	21,27	2,53
Dur	2168,71	101,69	546,64	74,77	36,44	4,98	22,79	3,12

Le lecteur aura déduit du tableau 11.3, outre les différences peu significatives entre les deux populations de 45 échantillons, que ce test s'est déroulé tard dans la nuit.

11.5.2.4. Dérive dans le temps

Partant du principe que 4 ou 5 mois constituaient une période de test suffisamment longue pour pouvoir déceler une éventuelle dérive dans le temps de la signature biométrique (nos 155 authentifications[G] étant réparties sur 20 semaines entre le 27.12.2002 et le 6.5.2003), nos avons tenté de déceler une éventuelle évolution de la distance relative. Le lecteur trouvera en ANNEXE 17 les courbes générées à partir d'un tableur excel (échelle de temps non linéaire).

L'allure de ces courbes ne semble pas devoir indiquer une tendance générale; en fait, elles sembleraient plutôt évoquer un biorythme.

11.5.3. Améliorations possibles

Les quelques expériences auxquelles nous nous sommes livrés n'ont bien entendu aucune valeur d'universalité, mais leurs résultats sont encourageants dans la mesure où:

- l'état de fatigue ne semble pas compromettre outre mesure la qualité de notre signature biométrique;
- le temps écoulé depuis l'enrôlement[G] ne semble pas compromettre outre mesure la qualité de notre signature biométrique;
- une différence au niveau de la sensibilité des claviers (de type identique) ne semble pas compromettre outre mesure la qualité de notre signature biométrique;
- sur 155 authentifications[G], deux seulement dépassaient le seuil de 34% de distance relative par rapport à la moyenne des enrôlements[G] tel que choisi par [Philippe-02].

Toutefois, nous ne pouvons ignorer la possibilité que la relative insensibilité de la signature biométrique par rapport aux facteurs envisagés puisse s'expliquer par le fait que l'évaluateur est un professionnel du clavier, aux automatismes bien ancrés; les résultats obtenus auraient peut-être été bien différents si nous avions demandé, pour ce test, le concours d'une personne moins rompue à la manipulation d'un ordinateur.

La technique d'identification[G] et d'authentification[G] biométrique présentée ici ne nous semble pas nécessiter d'amélioration particulière, mais uniquement les quelques mesures d'accompagnement que voici:

- cette technique doit venir en complément d'une identification[G] et authentification[G] traditionnelles;
- pour pouvoir fonctionner efficacement dans le cadre d'une application réseau, ce type d'authentification[G] doit être réalisée localement (prise d'empreinte) et la signature envoyée au

serveur pour analyse (puisque les clients ne conservent aucune données persistante), ce qui - à moins de combiner cette authentification[G] à un solution de chiffrement - présente une forte sensibilité au rejeu;

- nous ne pouvons pas exclure la possibilité que cette technique fonctionne moins bien - voire pas du tout - avec certains individus;
- enfin, l'enrôlement[G] de clients distants (et parfois très distants) pose un problème de logistique (envoi d'un logiciel pour réaliser l'enrôlement[G] ?) et de sécurité (retour des informations).

11.6. Conclusions

Nous avons repris au tableau 11.4 les différentes techniques d'identification[G] et d'authentification[G] qui ont été abordées dans ce chapitre et pour chacune d'entre elles, nous avons estimé sa conformité par rapport à certaines des mesures de protection issues des chapitres précédents. Cette estimation est basée sur une échelle simple à trois niveaux qui est la suivante:

- mesure non rencontrée: 0 point
- mesure partiellement rencontrée: 1 point
- mesure totalement rencontrée: 2 points

Tableau 11.4 Evaluation comparative des technologies envisagées

Ident.	*Libellé*	*PAP*	*CHAP*	*S/KEY*	*BIOM.*
(4.4.3.d)	Aucune donnée persistante (4.4.2.h) ne pourra transiter par un réseau autre que le réseau privé de l'entreprise. Sont visés ici, l'identité de l'utilisateur et son secret auquel nous assimilons la signature biométrique.	0	1	1	0
(4.4.3.e) *(4.7.3.d)*	Aucune donnée persistante (4.4.2.h) ne pourra être conservée sur une machine autre qu'un serveur du réseau privé de l'entreprise. Sont visés ici, l'identité de l'utilisateur et son secret.	2	2	2	2
(4.4.3.i) *(4.5.3.g)*	Les séquences d'identification et d'authentification (4.5.3.f) telles qu'elles peuvent être captées par un observateur sur le réseau doivent lui être inintelligibles (complètement chiffrées) (4.4.3.i) (4.5.1.g).	0	1	1	0
(4.5.3.h)	Les séquences d'identification et d'authentification (4.5.3.f) telles qu'elles peuvent être captées par un observateur sur le réseau ne pourront pas être rejouables (4.5.1.h)	0	2	2	0
(4.5.3.j)	Il ne doit pas être possible à une tierce personne présente sur le réseau d'usurper l'identité d'un utilisateur identifié et authentifié (4.5.1.j) (4.5.1.k) (ce qui sous-entend, par exemple, la répétition de l'"identification et de l'authentification à intervalles réguliers).	0	1	0	0
Total		***2/10***	***7/10***	***6/10***	***2/10***

L'analyse rapide de ce tableau nous conduit aux trois observations que voici:

- *(11.6.a)* CHAP semble être le type de protocole qui se positionne le mieux par rapport à nos exigences;
- *(11.6.b)* la plus grande faiblesse des 4 protocoles, à des degrés divers il est vrai, tient au fait qu'à un moment ou un autre des informations sont échangées en clair (non chiffrées);
- *(11.6.c)* l'authentification[G] biométrique nous paraît toujours intéressante parce que complémentaire à une authentification[G] traditionnelle comme CHAP, puisqu'elle met l'utilisateur relativement à l'abri d'une compromission de son secret qui serait due à une négligence de sa part (ce que nous appellerions le *syndrome du post-it*).

Chapitre 12 Chiffrement

Chiffrement: opération par laquelle on chiffre un message. **Chiffrer**: écrire, noter en chiffre, en un code conventionnel et secret. **Chiffre**: caractère numérique ou d'une écriture de convention employé dans une écriture secrète. (*Petit Robert*)

12.1. Introduction

12.1.1. Motivation

Un autre aspect plusieurs fois évoqué dans les chapitres précédents est le besoin d'avoir recours à des techniques de chiffrement dans le but de garantir la confidentialité[G] des messages[160] de notre application, que ces messages concernent l'authentification[G] des utilisateurs (11.6.b), la gestion du répertoire ou les conversations.

Nous avons vu qu'un protocole comme RTP offrait en interne une possibilité de chiffrement, possibilité que nous avons estimée peu satisfaisante. De même, la plupart des protocoles d'identification[G] et d'authentification[G] que nous avons évoqués pèchent par un défaut au moins partiel de chiffrement. Puisque les possibilités de chiffrement internes aux protocoles que notre application requiert (et que par rapport à elle nous qualifierions donc d'*endogènes*) ne nous donnent pas entière satisfaction, il nous paraît utile d'envisager de rechercher des protocoles ou outils qui permettraient de chiffrer efficacement les messages de notre application d'une manière *exogène*, c'est-à-dire en faisant appel à des ressources extérieures à celles qui la constituent.

Dans ce chapitre, notre attention se portera donc prioritairement sur les solutions (protocoles) permettant le chiffrement des messages, et non sur une analyse des algorithmes.

12.1.2. Principe

Le chiffrement consiste à transformer un message intelligible en un cryptogramme (inintelligible) en vue de son transfert via un medium non sécurisé. Arrivé à destination, le cryptogramme est déchiffré et le message intelligible délivré à son destinataire.

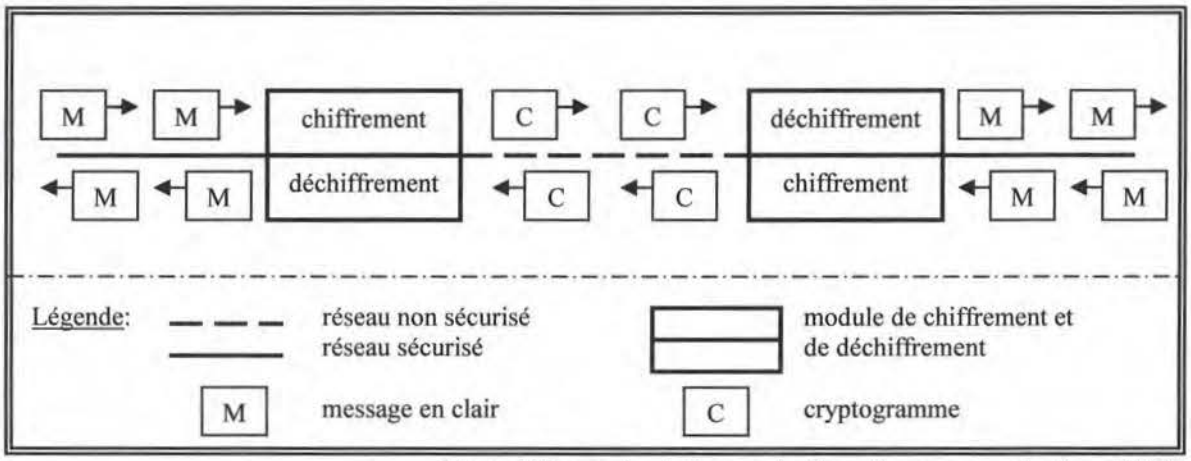


Figure 12.1: représentation symbolique d'une communication chiffrée (émetteur et récepteur non représentés)

[160] C'est la confidentialité qui nous intéresse au premier chef ici.

Conceptuellement, le chiffrement est affaire d'algorithmes mis en œuvre par des protocoles. Nous pouvons donc tenter une classification grossière des différents protocoles permettant un chiffrement selon deux critères très simples:

- le type d'algorithme utilisé et
- leur position dans le modèle de référence (OSI ou TCP/IP).

12.1.3. Méthode

Après avoir présenté les principaux types d'algorithmes, nous nous pencherons à nouveau sur notre modèle de référence (TCP/IP) par rapport auquel nous positionnerons quelques protocoles permettant d'échanger des informations de manière chiffrée. Le choix des protocoles représentés, basé sur leur notoriété, est un choix qui comporte une part de subjectivité puisque nous n'avons pas établi au préalable une liste exhaustive des candidats à notre investigation; nous estimons néanmoins qu'en choisissant au moins un protocole pour chacun des niveaux du modèle de référence sélectionné, nous effectuons un premier balayage satisfaisant des possibilités et techniques existantes.

Chacun des protocoles sélectionnés sera alors très rapidement présenté (principes généraux) puis rapidement évalué. Cette évaluation ne sera pas nécessairement une évaluation absolue, destinée à mettre en évidence les forces ou faiblesses intrinsèques du protocole en question, mais une évaluation relative à nos besoins propres.

12.2. Chiffrement et types d'algorithmes

12.2.1. Introduction

Du point de vue des algorithmes, la cryptographie moderne se caractérise souvent par l'utilisation d'algorithmes publics (le code en est connu) utilisant un secret (ou clé de chiffrement, c'est-à-dire une chaîne de caractères) pour transformer un message en cryptogramme, et inversement. Ces algorithmes se répartissent en deux catégories principales: ceux dont le secret est partagé[161] (les deux interlocuteurs doivent le connaître: on parle de cryptosystèmes symétriques) et ceux dont le secret n'est pas partagé (on parle alors de cryptosystèmes asymétriques). En plus de ces deux catégories existent un certain nombre d'algorithmes de chiffrement non réversibles: les algorithmes de hachage.

12.2.2. Les cryptosystèmes symétriques

Dans le chiffrement à clé symétrique, une même clé (secret partagé) est utilisée pour chiffrer le message à l'émission et le déchiffrer à la réception. Au plus longue la clé, au meilleure la sécurité (confidentialité[G]).

Les algorithmes à secret partagé sont plus efficaces en termes de performances (ils sont moins complexes) mais présentent quelques inconvénients parmi lesquels nous mentionnerons simplement le besoin initial de communiquer le secret à l'autre partie et le fait de devoir conserver ce secret à deux endroits différents (vulnérabilité[G] accrue).

Les algorithmes de chiffrement à clé partagée les plus souvent utilisés sont probablement DES (et ses variantes), RC2/RC5, IDEA et AES.

12.2.3. Les cryptosystèmes asymétriques

D'un autre coté les algorithmes de chiffrement à clé asymétrique, s'ils sont plus complexes (donc plus lents) ne présentent pas ces inconvénients. Avec ces algorithmes, chaque entité génère deux clés distinctes mais mathématiquement liées d'une manière telle que tout ce qui est chiffré par l'une pourra être déchiffré par l'autre uniquement, et inversément. Une des deux clés est alors gardée secrète (localement) tandis que l'autre, publique, est transmise à tous les interlocuteurs potentiels (par exemple par sa publication à l'aide de serveurs Internet spécialisés comme un numéro de téléphone est publié dans un bottin). Tout message peut alors être chiffré avec la clé publique de son destinataire, lequel sera le seul à pouvoir le déchiffrer parce que le seul à

[161] Par exemple, le protocole CHAP du chapitre précédent utilise un secret partagé.

détenir la clé privée correspondante (confidentialité[G]). Inversément, un message chiffré avec la clé privée de l'émissaire et donc déchiffrable par toute personne disposant de la clé publique correspondante constituera un élément efficace d'authentification[G] de l'origine (au sens 'possesseur de la clé privée correspondante') (imputabilité[G]).

L'algorithme de chiffrement à clé asymétrique (ou à clé publique) le plus utilisé est probablement celui développé par RSA.

12.2.4. Les fonctions de hachage

Une fonction de hachage (parfois appelée fonction sécurisée de hachage) est un moyen de prendre une empreinte digitale d'un message. Une telle fonction doit satisfaire les exigences suivantes:

- elle doit pouvoir générer un 'digest' de taille fixe à partir d'un message de taille quelconque;
- elle doit être reproductible (les mêmes causes produisant les mêmes effets);
- elle doit être non prévisible (petits changements, grands effets);
- elle doit être irréversible.

Les deux algorithmes les plus largement utilisés sont:

- MD5 (RSA Data Security, Inc; décrite dans [RFC1321]): génère un digest de 128 bits;
- SHA (US Government-developed Secure Hash Algorithm): génère un digest de 160 bits.

SHA est normalement 2^{32} fois plus sûr que MD5; mais à son désavantage, il traîne la réputation d'être un algorithme développé par la NSA, et d'être sensiblement plus lent que MD5.

12.2.5. Combinaisons

Plusieurs combinaisons des techniques évoquées ci-dessus s'avéreront extrêmement utiles puisqu'elles permettent l'établissement d'une clé symétrique, la signature digitale et l'enveloppe digitale.

Pour *établir une clé de chiffrement symétrique*, deux entités disposant chacune d'une paire de clé (cryptosystème asymétrique) pourront dans un premier temps s'échanger leur clé publique puis, en chiffrant leurs messages avec la clé publique de l'autre, négocier une clé de chiffrement symétrique. Tous leurs échanges consécutifs seront chiffrés avec la clé symétrique, plus efficace (en termes de performances).

La *signature digitale* consiste simplement, pour une entité émettrice d'un message, à générer un *digest* du message qu'elle s'apprête à envoyer (à l'aide d'une fonction de hachage) puis à chiffrer ce *digest* avec sa clé privée (cryptosystème asymétrique) avant de l'envoyer avec le message.

A la réception, l'entité destinataire générera son propre *digest* du message reçu en utilisant le même algorithme de hachage et comparera le résultat avec le *digest* reçu qu'elle aura préalablement déchiffré à l'aide de la clé publique de l'émetteur. Si les deux *digests* sont identiques, elle pourra en déduire que le message, même non chiffré, n'a pas été altéré (intégrité[G]) et qu'il provient bien d'une entité détenant la clé privée dont elle a utilisé la soeur publique pour déchiffrer le *digest* reçu.

L'*enveloppe digitale* est une technique consistant à chiffrer un message (clé symétrique) et à envoyer la clé en même temps que le message (clé symétrique chiffrée avec la clé asymétrique publique du destinataire). A la réception, la clé asymétrique privée correspondante est utilisée pour déchiffrer la clé symétrique qui est utilisée pour déchiffrer le message.

12.2.6. Possibilités d'authentification

Jusqu'à présent nous avons vu que le niveau d'authentification[G] que permettait l'utilisation des cryptosystèmes asymétriques se limitait à la certitude qu'un message reçu émanait bien d'une entité disposant de la clé privée correspondant à la clé publique utilisée pour le déchiffrer. Mais pour être sûr que le possesseur de cette clé privée est bien l'entité qu'il prétend être, nous avons besoin qu'il nous montre une pièce d'identité établie par un tiers de confiance.

En d'autres mots, si *A* et *B* ne se connaissent[162] pas mais connaissent tous les deux *C*, c'est *C* qui pourra garantir à *A* que la clé publique *Pb(B)* appartient bien à *B*, et à *B* que la clé publique *Pb(A)* appartient bien à *A*. Bien sûr, en pratique, *C* ne va pas intervenir directement sous cette forme, mais c'est lui qui va délivrer à *A* et à *B* une pièce d'identité (un certificat) digitalement signé de sa main [12.2.5]. Dans cet exemple, *C* devient ce qu'on appelle une *autorité de certification* (CA); les différentes CA sont organisés en une structure pyramidale, chaque CA d'un niveau supérieur certifiant l'identité d'un ou de plusieurs CA d'un niveau inférieur, jusqu'au sommet de la pyramide où se trouve la *root certification authority*.

12.3. Chiffrement et modèle de référence

Par rapport au modèle de référence TCP/IP, un chiffrement pourra par exemple être opéré au niveau de la couche 1 (sécurité des liaisons), des couches 2 ou 3 (sécurité des communications), ou encore en couche 4 (sécurité des applications).

Un chiffrement en couche 1 TCP/IP (hôte - réseau) pourra être implémenté en hardware ou en software mais concernera tout le trafic de tous les protocoles de communication des couches supérieures, charge utile et en-têtes comprises. Non seulement cela peut ne pas s'avérer nécessaire, mais en plus il sera nécessaire de déchiffrer systématiquement les cryptogrammes à chaque fois par exemple qu'une décision de routage devra être prise. Pour palier cet inconvénient dans un univers de réseaux hétérogènes interconnectés, on a souvent recours à des techniques d'encapsulation: par exemple, le flux de niveau 1 peut-être chiffré et encapsulé dans de l'IP (niveau 2), ce qui lui permet de naviguer d'un réseau privé à un autre à travers le réseau public et ses différents protocoles. Etant donné que les utilisateurs potentiels de notre SC sont distribués sur l'Internet, un protocole de ce niveau qui ne réaliserait pas cette encapsulation n'aurait aucune chance de nous intéresser.

Un chiffrement au niveau 2 TCP/IP (internet: IP) permet de chiffrer tout le trafic de la couche supérieure (transport) que s'échangent deux systèmes. Etabli au niveau 3 TCP/IP (transport: TCP, UDP, ...) le chiffrement est alors dit de *processus à processus* et peut donc ne concerner qu'une partie des flux que s'échangent les deux systèmes.

Pour terminer, un chiffrement en couche 4 TCP/IP (application) pourrait ne concerner que certains échanges bien particuliers d'une application (par exemple, le chiffrement du seul transfert d'un mot de passe ou d'un numéro de carte de crédit vers un site Internet).

Parmi les nombreux protocoles des différentes couches de notre modèle de référence TCP/IP qui permettent d'établir des flux chiffrés, nous avons repris et positionné au tableau 12.1 ceux qui nous paraissaient les plus connus.

Tableau 12.1	**Exemples de protocoles réalisant le chiffrement des informations et positionnement en fonction des modèles OSI et TCP/IP** [Tanenbaum-97]			
OSI		*TCP/IP*		*Protocoles*
Couche	*N.*	*N.*	*Couche*	
Application	7	4	Application	SSH, S/MIME, SIP
Présentation	6			
Session	5			
Transport	4	3	Transport	SSL/TLS
Réseau	3	2	Internet	IPSec (AH/ESP)
Liaison de données	2	1	Hôte - Réseau	L2TP
Physique	1			

12.4. Chiffrement au niveau 1 (TCP/IP): L2TP

12.4.1. Principe

L2TP (Layer 2 Tunneling Protocol) est un protocole de communication non fiable orienté connexion destiné à permettre l'encapsulation des trames PPP pour leur permettre de traverser des réseaux hétérogènes interconnectés de manière transparente pour les utilisateurs et applications concernés (figure 12.2). Il permet

[162] "Connaître *X*" signifie "avoir la certitude que c'est bien *X* qui détient la clé privée *Pv(X)*".

donc de prolonger une connexion PPP au-delà du serveur d'accès de l'ISP jusqu'au serveur d'accès du réseau privé auquel l'utilisateur du poste client souhaite se connecter.

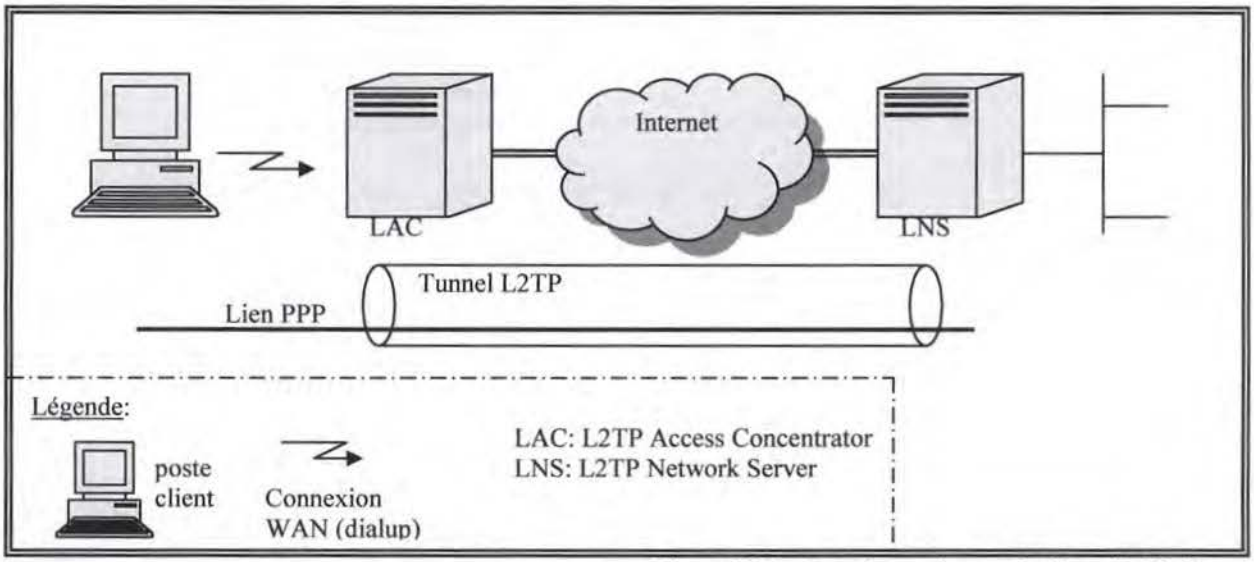


Figure 12.2: Représentation symbolique de L2TP

L2TP réalise l'encapsulation des trames PPP en fonction du type de protocole réseau rencontré, qui est souvent IP (voir l'exemple de la figure 12.3) mais pas nécessairement. L2TP lui-même comprend deux types de charge utile: il peut transporter des messages applicatifs (trame PPP) mais aussi des messages de contrôle pour ses propres besoins (établissement des connexions, etc.).

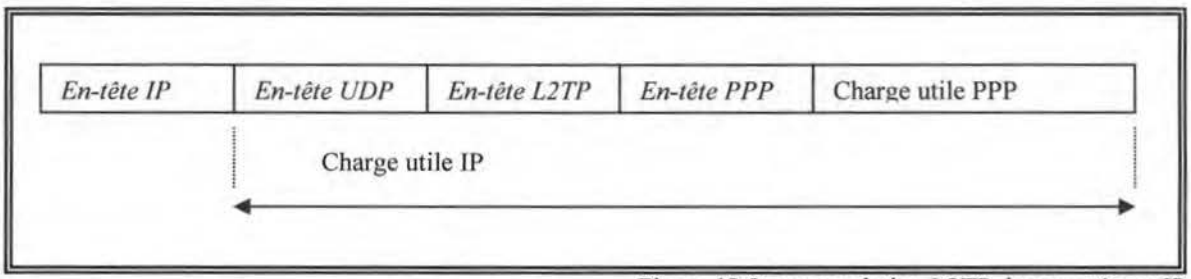


Figure 12.3: encapsulation L2TP dans un réseau IP

12.4.2. Evaluation

Le protocole L2TP permet une authentification[G] mutuelle selon le mode CHAP pour les deux extrémités du tunnel lors de son établissement, mais il n'y a pas d'authentification[G] au niveau de chaque trame, ce qui le rend vulnérable à des attaques de type *man in the middle*[G]. Il n'y a pas non plus de garantie d'intégrité[G] au niveau de ces trames (risque[G] d'attaque de type *DoS*[G] envers les messages de contrôle) et, de plus, L2TP n'offre pas vraiment de possibilité de chiffrement en soi puisqu'en réalité seule la charge utile PPP peut être chiffrée - mais PPP ne fournit pas grand chose comme possibilités de négociation, d'échange ou de rafraîchissement de clés.

La plupart du temps, L2TP se reposera donc sur les possibilités de chiffrement du protocole encapsulant de couche 2 TCP/IP (internet).

12.5. Chiffrement au niveau 2 (TCP/IP): IPSec

12.5.1. Principe

IPSec est un ensemble de protocoles pouvant offrir en mode non connecté des garanties de confidentialité[G], d'intégrité[G] et d'imputabilité[G] (authentification[G]) au niveau 2 TCP/IP (IP). Il est parfois présenté comme un protocole à deux niveau, le niveau inférieur (couche 2 TCP/IP: internet) offrant la plupart des garanties

mentionnées tandis qu'un niveau supérieur (couche 4 TCP/IP: application) prend en charge les aspects de négociation et d'échange de clés ou de certificats.

Lors de l'initialisation d'IPSec, un premier protocole de niveau 4 TCP/IP (IKE) se charge d'authentifier les différentes parties et de leur fournir du matériel pour générer (et par la suite rafraîchir) des clés de chiffrement. Les garanties mentionnées dans le paragraphe précédent sont apportées ensuite grâce à l'aide du protocole AH, du protocole ESP ou d'une combinaison des deux (protocoles de niveau 2 TCP/IP).

Quelque soit le protocole utilisé (AH ou ESP), IPSec peut être utilisé selon un des deux modes suivants:

- en mode *transport*, AH ou ESP se contentent d'ajouter son (ses) bloc(s) d'informations devant (ou autour de) la charge utile du datagramme IP d'origine, alors que
- en mode *tunnel*, IPSec réalise une encapsulation *IP over IP*, après que AH ou ESP ait ajouté son (ses) bloc(s) d'informations devant (ou autour de) la charge utile du datagramme IP d'origine.

Le mode *tunnel* est utilisé lorsque l'intégrité[G] des champs modifiables[163] de l'en-tête du datagramme IP d'origine doit être garantie: l'ensemble du datagramme est alors encapsulé dans un nouveau datagramme IP.

AH ajoute un en-tête (24 octets minimum) comportant plusieurs champs parmi lesquels nous ne mentionnerons que ceux qui nous intéressent au premier chef, à savoir:

- un numéro de séquence garantissant la protection contre le rejeu,
- un total de contrôle calculé sur l'ensemble des champs du datagramme IP (en-tête et charge utile) à l'exception des champs modifiables de l'en-tête IP actif, garantissant l'intégrité[G] et, partant, l'origine comme la destination (puisque les adresses IP, authentifiées par IKE, sont couvertes par ce total de contrôle).

AH en mode *transport*: le total de contrôle de l'en-tête AH couvre l'ensemble du paquet à l'exception des champs modifiables de l'en-tête IP.

En-tête IP	*En-tête AH*	Charge utile IP

AH en mode *tunnel*: le total de contrôle de l'en-tête AH couvre l'ensemble du paquet à l'exception des champs modifiables du premier en-tête IP (l'en-tête *actif*).

En-tête IP	*En-tête AH*	*En-tête IP*	Charge utile IP

Figure 12.4: AH (*Authentication Header*)

ESP fonctionne sur base du même principe, mais là où AH ajoutait un seul bloc d'en-tête, ESP ajoute un bloc d'en-tête, un bloc de fin et un bloc d'authentification[G]. L'en-tête (8 octets minimum) contient le numéro de séquence, et le bloc d'authentification[G] contient le total de contrôle calculé sur l'en-tête ESP, la charge utile et le bloc de fin ESP[164] (y compris les adresses IP source et destination).

AH et ESP semblent redondants, mais quelques différences méritent d'être signalées:

- seul ESP permet le chiffrement;
- ESP requiert l'utilisation d'algorithmes de compression plus lourds que AH, avec les restrictions que cela peut impliquer pour certains pays;
- lorsque seules des garanties d'intégrité[G] sont demandées, AH est bien plus performant;

[163] Typiquement, des champs comme *Type of Service* (TOS), *Flags*, *Fragment Offset*, *Time to Live* (TTL) et le *checksum* sur l'en-tête.

[164] Le bloc de fin ESP contient des informations qui ne nous intéressent pas particulièrement ici, comme par exemple le nombre d'octets de remplissage ajoutés à la charge utile.

- la combinaison des deux protocoles permet un contrôle plus fin du réseau IPSec, mais ceci sort du cadre de ce document.

ESP en mode *transport*: le total de contrôle de ESP couvre l'ensemble des champs de l'en-tête ESP au bloc de fin inclus alors que seuls la charge utile et le bloc de fin ESP sont chiffrés.

En-tête IP	*En-tête ESP*	Charge utile IP	*Bl. fin ESP*	*Auth. ESP*

ESP en mode *tunnel*: le total de contrôle de ESP couvre l'ensemble de l'en-tête ESP au bloc de fin inclus, alors que seuls l'en-tête IP encapsulée, la charge utile et le bloc de fin ESP sont chiffrés

En-tête IP	*En-tête ESP*	*En-tête IP*	Charge utile IP	*Bl. fin ESP*	*Auth. ESP*

Figure 12.4: ESP (*encapsulating security payload*)

12.5.2. Evaluation

IPSec est en passe de devenir la suite de protocoles incontournable pour la construction de VPNs, y compris pour la sécurisation des liaisons L2TP [RFC3193]. Par rapport à nos besoins, nous identifions toutefois un certain nombre d'éléments discordants:

- IKE permet une authentification[G] basée sur un échange de certificats, ce que nous ne requérons pas et qui de plus fait intervenir un tiers (11.1.1.b);
- le chiffrement est disponible avec ESP seulement, qui est habituellement décrit comme plus lent que AH (or notre application est de type interactif);
- IPSec, par défaut, relie deux machines; si nous souhaitons limiter l'utilisation de ce mode de transport (ou tunnel) à une seule application, une configuration plus poussée basée sur les numéros de ports est requise[165];
- lorsque deux LAN - au sein desquels des adresses IP privées sont utilisées - sont reliés par IPSec, les *end points* du protocole IPSec sont obligatoirement situés sur les machines réalisant le SNAT (dispositifs de protection logique)[166]; entre chaque poste client et le dispositif correspondant, aucun chiffrement ne protègera nos messages.

D'une manière générale, IPSec est présenté comme un protocole relativement lourd et complexe dont le plus gros avantage, puisqu'il fonctionne principalement au niveau 2 TCP/IP, est d'être transparent pour les utilisateurs et les applications. D'aucuns lui reprochent parfois aussi de ne réaliser que l'authentification[G] des systèmes (puisque nous sommes au niveau 2 TCP/IP) mas cela nous convient assez; par contre, ce protocole étant relativement récent[167], la disponibilité et l'interopérabilité de ses implémentations dans la version 4 du protocole IP (IPv4) semblent parfois poser quelques problèmes.

En conclusion, nous dirions que IPSec est assurément un bel outil promis à un riche avenir, mais qui ne semble pas particulièrement adapté à nos besoins.

12.6. Chiffrement au niveau 3 (TCP/IP): SSL/TLS

12.6.1. Principe

SSL fut à l'origine développé par Netscape, mais est maintenant intégré dans pratiquement tous les navigateurs et serveurs web. SSL utilise les techniques vues en introduction de ce chapitre (chiffrement à clé symétrique et asymétrique, signature digitale, certificats publics) pour atteindre ses objectifs qui sont:

[165] Pour peu qu'ils puissent être connus à l'avance.
[166] S'il en était autrement, puisque le total de contrôle est calculé aussi sur les champs *adresse* de l'en-tête IP, le changement de l'adresse IP source ou *source natting* (SNAT) poserait quelques problèmes.
[167] Et par ailleurs composante indissociable de la version 6 du protocole IP (IPv6).

- assurer la confidentialité[G] des échanges
- assurer l'intégrité[G] des échanges
- assurer l'authentification[G]; habituellement, seule l'authentification du serveur est effectuée et nous ne considérerons que ce cas de figure ici (fonctionnement *asymétrique*), mais SSL permet d'effectuer également l'authentification du client.

Par rapport au modèle de référence TCP/IP, SSL se situe plus exactement entre la couche *Transport* (TCP) et la couche *Application* (figure 12.5), ce qui le rend presque transparent pour les utilisateurs[168], et apparaît fonctionnellement comme constitué de deux parties:

- l'établissement de la session (*handshake protocol*: on se présente et on négocie les options) et
- la session (*record protocol*).

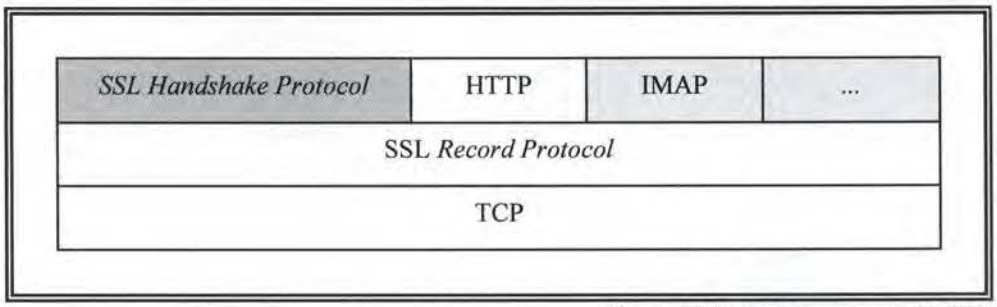


Figure 12.5: Positionnement de SSL

Le *handshake protocol* de SSL a donc pour objectif l'initialisation de la connexion (négociation des modes cryptographiques et de leurs options) et l'authentification[G]; il se déroule comme suit:

- le client envoie un HELLO message au serveur; ce message contient:
  - la version de SSL supportée par le client,
  - la liste des options / protocoles de chiffrement / compression supportés par le client et
  - un nombre aléatoire;
- le serveur répond au client par un message HELLO qui contient:
  - le même genre d'informations que celles reçues du client plus
  - son certificat contenant sa clé publique et signé par une CA;
- le client répond par un message chiffré avec la clé publique du serveur, et qui contient:
  - une 'proto clé' (autre nombre aléatoire) et
  - une requête pour passer en mode chiffré.
- Séparément, le client et le serveur utilisent une fonction de hachage impliquant les deux nombres aléatoires (messages 1 et 3), dont ils tirent une clé qui sera symétrique[169]; cette clé n'est donc jamais envoyée telle quelle;

Tous les messages qui suivent sont maintenant établis comme suit (*record protocol*):

- utilisation du hachage pour générer un *digest*, garant de l'intégrité[G] du message;
- l'ensemble (message et *digest*) est chiffré avec la clé symétrique;
- envoi de l'ensemble.

12.6.2. Evaluation

SSL est un des protocoles de sécurité les plus utilisés et à ce titre considéré par certains comme un des plus éprouvés. Et effectivement, la plupart des problèmes de sécurité impliquant SSL sont liés à des problèmes ou caractéristiques de l'implémentation[170] . Même si, outre ces traditionnels *buffer overflow* et autres erreurs

[168] Une application qui souhaite faire appel à SSL doit être conçue pour cela (*SSL enabled*, comme HTTPS ou IMAPS), ce qui n'était pas le cas avec IPSec.

[169] En réalité plusieurs clés sont dérivées, mais ce détail n'apporte rien à la compréhension du principe de base.

[170] Une rapide recherche dans la base de connaissance du CERT (http://www.kb.cert.org/vuls) nous fournit des exemples de vulnérabilités d'implémentations connues: mod_ssl (http://www.modssl.org), Apache_SSL (http://www.apache.group), OpenSSL (http://www.openssl.org), Internet Explorer (http://www.microsoft.com).

d'implémentation, quelques attaques très techniques ont parfois permis de découvrir tantôt le mot de passe d'une session IMAP4 (http://lasecwww.epfl.ch/memo_ssl.shtml), tantôt une clé privée, le niveau d'expertise que de telles attaques requièrent est très élevé et peu compatible avec l'attrait qu'une cible comme notre application pourrait représenter.

Par rapport à nos besoins particuliers, SSL nous intéresse donc particulièrement pour les raisons suivantes:

- des implémentations portables (windows et unix) existent qui nous permettraient, en cas de besoin, d'encapsuler facilement tout le trafic de notre application et ce trafic là seulement (http://www.stunnel.org);
- le code source de la plupart de ces implémentations est disponible (GPL), ce qui devrait permettre, en cas de développement, une intégration du *handshake protocol* à notre application (couche 4 TCP/IP);
- SSL est en soi un protocole qui peut, via le port habituel 443/tcp (HTTPS), franchir la plupart des dispositifs de protection logique, et en conséquence
- l'utilisation de SSL permettrait à nos mécanismes d'identification[G] et d'authentification[G] d'échanger tous leurs messages de *processus à processus* de manière chiffrée.

Toutefois, nous ne pouvons pas ne pas prendre en considération les éléments suivants:

- SSL introduirait un coût supplémentaire pour ce qui est des communications:
  - il utilise tcp (transport fiable, ce qui n'est pas requis) et
  - il garantit l'intégrité[G] (hachage);
- SSL permet une authentification[G] basée sur un échange de certificats, ce que nous ne requérons pas et qui de plus fait intervenir un tiers (11.1.1.b). Mais cela ne nous paraît pas incontournable.

12.7. Chiffrement au niveau 4 (TCP/IP): SSH

12.7.1. Principe

Résolument positionné au niveau application (couche 4 TCP/IP), SSH fut historiquement conçu comme une version sécurisée des *R-commandes* (rsh et rlogin) avec comme objectifs principaux:

- éviter la compromission des mots de passe, qui circulent *en clair* sur le réseau;
- disposer d'une authentification[G] renforcée des machines, pas seulement basée sur le nom ou l'adresse IP;
- pouvoir exécuter en toute sécurité des commandes à distance;
- pouvoir transférer des fichiers en toute sécurité;
- sécuriser les sessions X11.

SSH apporte une réponse à tous ces objectifs, mais malheureusement avec des différences significatives entre les versions 1.x et 2.x, incompatibles entre elles.

Lors de l'établissement initial d'une connexion, SSH se comporte d'une manière similaire à SSL[171] pour l'établissement d'une clé de chiffrement symétrique qui sera utilisée par la suite[172]. Une fois cette clé en place, l'identification de l'utilisateur peut avoir lieu (les procédés disponibles dans SSH pour l'identification[G] et l'authentification[G] des utilisateurs comprennent PAP, S/KEY, CHAP et l'authentification[G] par clé asymétrique). A partir de ce moment, un tunnel SSH est créé qui peut être emprunté par plusieurs applications différentes.

[171] L'implémentation Unix, OpenSSH, utilise d'ailleurs les librairies OpenSSL. SSH ne fait toutefois pas appel aux certificats.
[172] A partir de SSH 2.x, plusieurs clés sont négociées (comme dans SSL).

12.7.2. Evaluation

SSH est très populaire et fort répandu mais souffre d'un certain nombre de handicaps dont nous citerons, à titre d'exemple:

- les incompatibilités entre versions 1.x et 2.x (implémentant les versions 1 et 2 du protocole);
- le passage du modèle *open source* au modèle commercial pour la distribution officielle et à partir de l version 2;
- certaines curiosités particulières de l'implémentation open source majeure (OpenSSH), comme par exemple le fait qu'elle utilise (via lien dynamique) la librairie OpenSSL qu'elle aura trouvé sur la machine;
- la possibilité d'exploitation d'un canal caché (utilisation d'octets de remplissage dont les valeurs ne sont pas prévisibles);
- tout le protocole étant implémenté au niveau 4 TCP/IP (application), son utilisation n'est pas transparente du tout pour l'utilisateur.

12.8. Chiffrement au niveau 4 (TCP/IP): S/MIME

12.8.1. Principe

MIME est un protocole de description de contenu permettant de décrire le format des données transportées dans le corps d'un message[173] internet, mais aussi de mélanger, dans un seul et même message, plusieurs types d'objets.

S/MIME, la version *Secure* de MIME, peut mettre en oeuvre un cryptosystème asymétrique qui lui permet d'ajouter à MIME des possibilités d'authentification[G], de garantie d'intégrité[G], de confidentialité[G] et de signature digitale.

Au niveau de l'en-tête du message, la version de MIME utilisée (exemple: *MIME-Version: 1.0*) et le type de format du message sont renseignés (exemple: *Content-Type: type / sous-type*[174]). Lorsqu'un type de contenu 'multipart' est indiqué, une chaîne de caractères aléatoire est choisie comme séparateur des différents types de contenu du message (exemple: *Content-Type: multipart / mixed; boundary = "SomeRandomString"*) et chaque partie commencera par la spécification de son propre *Content-Type*.

En plus de tous les types de contenu définis par MIME (par exemple audio/x-wav), S/MIME en ajoute un certain nombre parmi lesquel figurent des Content-type comme "data", "signedData", "envelopedData", "signedAndEnvelopedData", "digestedData", et "encryptedData". A ce titre, les données sécurisées sont toujours des données 'MIME', et la protection ne concerne donc qu'une partie du message complet.

12.8.2. Evaluation

L'intérêt de S/MIME réside dans le fait qu'il peut être utilisé et/ou implémenté au niveau application; il permet donc, de manière très fine, de décider quelles informations doivent être protégées, et de ne protéger que celles-là. S/MIME permet aussi de transporter du contenu multimédia, mais il s'agit là principalement d'un transport à des fins de diffusion, puisqu'aucun des mécanismes de codage ni de contrôle et d'adaptation des flux aux performances mesurées, mécanismes que nous avons évoqués avec RTP/RTCP, n'existe ici. S/MIME peut donc représenter une bonne solution à intégrer dans d'autres protocoles pour y ajouter juste ce qu'il faut de chiffrement ou de signature digitale (par exemple, pour chiffrer une phase critique), mais il ne devrait pas être fort utile dans une application comme celle que nous projetons.

---

[173] MIME était initialement destiné à permettre l'enrichissement des types de données véhiculés par les courriers électroniques (protocole SMTP), mais est maintenant utilisé par de nombreux autres protocoles (par exemple HTTP, mais aussi SIP/SDP dont nous avons parlé).

[174] La syntaxe est plus riche que cet exemple le laisse à penser, puisque des paramètres peuvent être ajoutés (exemple: *Content-Type: text/plain; charset=ISO-8859-1*).

12.9. Conclusions

Nulle part ailleurs dans ce document nous n'avons autant simplifié et résumé les choses que dans ce chapitre consacré au chiffrement, mais c'était peut-être le prix à payer pour éviter d'y consacrer une partie entière de ce travail. Ce survol, pour rapide qu'il fut, nous a toutefois permis de nous éclairer quelque peu sur les possibilités de chiffrement exogènes.

Premier enseignement, le niveau par rapport au modèle de référence. Au plus bas, au moins de discernement sur ce qui doit ou ne doit pas être chiffré, mais aux niveaux supérieurs apparaît le problème de la complexité d'implémentation (en cas d'intégration dans le code du SC) ou de la transparence pour les utilisateurs. Comme notre intention est de chiffrer l'entièreté du trafic pour une application, le bon niveau semble être celui auquel SSL se trouve.

Deuxième enseignement, la difficulté d'éviter les risques[G] d'une attaque du style *man in the middle*[G]. En effet, l'authentification[G] au niveau du datagramme semble constituer la meilleure prévention contre ce genre d'attaque, mais il est difficile de garantir l'origine d'un datagramme (via une somme de contrôle portant sur une partie de l'en-tête IP) lorsque son adresse source est modifiée lors du passage en sortie au travers des dispositifs de protection logique (SNAT).

Troisième et dernier enseignement majeur, certains protocoles (comme SSL), lorsqu'ils sont intégrés dans une application (comme HTTPS) permettent de traverser la plupart des dispositifs de protection logique puisque le port qu'ils utilisent est pratiquement ouvert partout en sortie (directement ou via *proxy* http).

Cinquième partie LE SYSTEME

Les éléments issus des chapitres précédents nous permettent de dessiner notre application telle que nous la développerions. De cet exercice, nous dégagerons un certain nombre de critères d'évaluation que nous appliquerons à quelques produits connus, évaluation qui nous aidera à décider du mode d'acquisition de notre SC.

Chapitre 13 Catalogue des exigences

Ce chapitre vise à reprendre, organiser et définir un jeu minimum d'exigences par rapport au SC. Le cas échéant, c'est sur cette base que nous entamerions le processus complet de spécification et de développement.

13.1. Généralités

13.1.1. Motivations

Les objectifs généraux à l'origine du projet tels qu'ils ont été identifiés au chapitre 2 peuvent être résumés comme suit:

- *(13.1.1.a)* réduction des frais téléphoniques (2.1.1.b);
- *(13.1.1.b)* réduction de la superficie de bureaux occupée par le recours au télétravail (2.1.1.c);
- *(13.1.1.c)* développement des synergies internes (collaboration entre employé distants) (2.1.2.a);
- *(13.1.1.d)* amélioration de la qualité du support (2.1.3.b).

13.1.2. Finalité du système

Le SC, tel qu'il a été présenté sous l'angle de ses objectifs concrets dans la première partie de ce document, devra permettre la communication vocale entre personnes distantes via l'Internet (2..2..b) *(13.1.2.a)*. Cette finalité, qui a été précisée ensuite au niveau opérationnel (3.1), correspond à la fonction de communication F_COMM telle que présentée dans la deuxième partie de ce document (5.2.3.3.a).

13.1.3. Le système et son environnement

Les relations entre le SC et son environnement ont été envisagées dans la deuxième partie de ce document (4.6), et l'identification du SC par rapport à son environnement a été illustrée par la figure 5.3 (5.2.3.2). Du paragraphe précité, nous retiendrons la découpe du SC en trois parties : les sous-systèmes *serveur* (5.2.3.2.a), *client* (5.2.3.2.b) et *distants* (5.2.3.2.c) *(13.1.3.a)*.

13.1.4. Hypothèse simplificatrice

Au vu des chapitres qui précèdent et avant d'organiser nos exigences, il nous semble opportun d'introduire une petite simplification que voici: considérant que le mode *conférence* (3.1.c), pour utile qu'il soit, ne

représentera jamais qu'une exception dans l'utilisation quotidienne du SC, nous estimons défendable et intéressant de ne plus considérer la possibilité d'exploiter le SC en mode IP *multicast*[G] *(13.1.4.a)*[175].

13.2. Acteurs, fonctions sujets et objets du système

13.2.1. Acteurs du système

Les (types d') acteurs sont au nombre de quatre et répartis comme suit:

- *(13.2.1.a)* un type d'acteur principal: les utilisateurs humains (3.2.a) (3.2.b);
- *(13.2.1.b)* un type d'acteur secondaire: l'administrateur (3.2.c) et le développeur;
- *(13.2.1.c)* un autre système: les ressources de l'environnement (4.6.2);
- *(13.2.1.d)* le SC lui-même.

13.2.2. Fonctions du système

Les principales fonctions[176] du SC peuvent être réparties en trois catégories : les fonctions accessibles aux utilisateurs, les fonctions réservées à l'administrateur et les fonctions internes.

Les fonctions exploitées par les utilisateurs sont celles qui relèvent de la finalité du SC (13.1.2.a):

- F_AUTH : l'identification[G] et l'authentification[G] des utilisateurs (3.3.2),
- F_REPER : la gestion du répertoire (3.3.3),
- F_INVIT : la gestion des invitations[G] (3.3.4) et
- F_SESS : la gestion des sessions[G] (3.3.5).

Les fonctions réservées à l'administrateur sont:

- F_ENROL (5.2.3.3.b): la gestion des utilisateurs, ou enrôlement[G] (3.3.6.a), et
- F_ADM : le suivi de l'exploitation (configuration, gestion de l'audit, ...) (3.3.6..b).

Les principales fonctions internes relatives à la sécurité[177] sont :

- F_ACTRL : le contrôle des droits d'accès des sujets[G] par rapport aux objets[G] et
- F_AUDIT : l'imputation des actions aux sujets[G] (génération de l'audit).

13.2.3. Fonctions périphériques au système

Plusieurs fonctions du SI de l'entreprise se situent en périphérie du SC mais n'en font pas à proprement parler partie; c'est la cas par exemple de:

- F_DEVEL (5.2.3.3.c) : le développement de l'application (auquel nous assimilons les phases d'analyse des risques[G], de spécification et de conception),
- F_DEPLO (5.2.3.3.d) : le déploiement de l'application et
- F_MAINT : la maintenance corrective et évolutive de l'application.

Nous n'avions pas encore introduit ce concept de maintenance (F_MAINT), considérant dans une première approche que celle-ci pouvait se résumer à une succession de phases de développement et de déploiement.

---

[175] L'exploitation occasionnelle du SC en mode conférence (3.1.e) se traduira donc par une consommation accrue de bande passante.

[176] Nous envisageons ici le terme *fonction* dans le sens plus précis d'*activité non technique* et non plus de *finalité opérationnelle* comme précédemment (13.1.2).

[177] Nous nous limitons volontairement, pour les fonctions internes, à celles relevant directement de la problématique de la sécurité; les autres fonctions internes relèvent davantage d'un document de conception que d'une ébauche de spécification d'exigences.

Mais les besoins de *journalisation de la maintenance* et de *suivi des patches et versions*, identifiés grâce à l'approche CEA (tableau 7.6, fiche 27), nous ont poussé à revoir cette position.

13.2.4. Sujets du système

Les acteurs (13.2.1) d'un SC en constituent habituellement le groupe des sujets[G] *(13.2.4.a)*. Observons toutefois que la plupart des sujets[G] peuvent également avoir un rôle d'objets[G] *(13.2.4.b)*.

13.2.5. Objets du système

Les objets[G] d'un SC sont également de nature variée: nous y retrouvons les fonctions du SC (13.2.2), les informations du SC (tableau 5.2) (5.2.3.3), les entités du SC (tableau 5.4) (5.2.4.1), ou encore certains concepts plus abstraits comme les notions de connexion[G] et de session[G]. Ici aussi, nous observons que certains objets[G], par exemple les fonctions sollicitées par les utilisateurs, peuvent agir en tant que sujets[G] par rapport à d'autres objets[G] (un objet[G] *fonction* peut créer ou détruire un objet *session*[G]).

13.3. Eléments de politique de sécurité

13.3.1. Sécurité physique

La sécurité physique de la salle des serveurs (sous-système *serveur* (13.1.3.a)) est réputée optimale (5.2.3.4.b) (7.4.2.s) (7.4.2.z) *(13.3.1.a)*. Le niveau de sécurité physique des sous-systèmes *local* et *distants* (13.1.3.a) est indéfini *(13.3.1.b)*.

13.3.2. Sécurité organisationnelle et administrative

La prise de conscience de la problématique de la sécurité au niveau de l'entreprise est réputée optimale (5.2.3.4.a) (7.4.2.v) (8.3.3.i) *(13.3.2.a)*. Le niveau de prise de conscience de la problématique de la sécurité au niveau des clients de l'entreprise (certains des sous-systèmes *distants* (13.1.3.a)) est indéfini *(13.3.2.b)*.

Au niveau de la sécurité administrative, la répartition des rôles (utilisateur, administrateur, développeur) au sein de l'entreprise est clairement établie et respectée *(13.3.2.c)*.

13.3.3. Sécurité logique externe

La sécurité logique externe au SC (dispositifs de protection logique des sous-systèmes *serveur* et *local* (13.1.3.a)) est réputée optimale (5.2.3.4.c) (7.4.2.aa) *(13.3.3.a)*. La sécurité logique externe des sous-systèmes *distants* (13.1.3.a) est indéfinie *(13.3.3.b)*.

13.3.4. Sécurité logique interne : droits et contrôles d'accès

Au niveau du SC, le modèle de contrôle d'accès[178] hérité de la classe de fonctionnalité F-C2 (8.3.2) est de type discrétionnaire [G]; toutefois, le type de notre SC, dans lequel les objets sont la plupart du temps manipulés par les fonctions du SC elles-mêmes[179] à l'instigation des utilisateurs, nous semble mieux se prêter au moins partiellement à un modèle mandataire[G] par ailleurs estimé plus sûr que le modèle discrétionnaire[G]. Hormis l'administrateur, les utilisateurs ne disposeraient donc d'aucune prérogative quant aux droits d'accès aux différents objets[G] du SC (8.3.2.h), et ce quand bien même ils seraient eux-mêmes à l'origine de la création de ces objets[G] *(13.3.4.a)*.

[178] Un modèle de contrôle d'accès implémente une politique de sécurité en définissant et régissant les droits des sujets sur les objets. Le besoin de classification et de contrôle d'accès des objets a été établi notamment par la méthode du CEA (7.4.2.w).

[179] C'est-à-dire par d'autres objets agissant en tant que sujets.

Pour illustrer ceci, nous dirions que l'approche discrétionnaire[G] nous pousserait par exemple à considérer que c'est l'utilisateur qui *crée*[180] une session[G] et donc, en tant que propriétaire de cette session[G], c'est lui seul qui détiendrait le droit d'invitation[G] à cette session, mais aussi le droit de transmettre ce droit d'invitation[G] à un autre utilisateur invité, ou encore le droit de mettre fin à la session[G]. D'une manière générale, ce genre d'approche souffre d'un gros handicap, que nous appellerions le problème de la transitivité: pour prendre une analogie simple, dans un système de fichiers implémentant ce genre de modèle, si l'utilisateur *X* donne à l'utilisateur *Y* le droit de lire l'objet[G] *O*, *Y* peut facilement copier *O* puis autoriser l'utilisateur *Z* à lire la copie.

Notre approche est légèrement différente et consiste à considérer que les utilisateurs ont le droit d'*utiliser* des fonctions, mais que pour le reste c'est le SC lui-même (éventuellement via configuration relevant du seul administrateur) qui décide des droits des sujets[G] sur les objets[G], et de les faire respecter. Cette approche, plus proche du modèle mandataire[G] que du modèle discrétionnaire[G], nous paraît plus simple à implémenter dans un SC du type de celui dont il est question ici, et est également plus proche de nos besoins; peu importe qui crée la session[G], celle-ci se termine quand plus personne ne l'utilise et si l'utilisateur *Y* a le droit de consulter les données signalétiques de l'utilisateur *Z*, il ne peut transmettre ce droit à personne - pas plus que celui de consulter ses propres données signalétiques[181].

13.4. Les exigences sur le système

13.4.1. Introduction

Les paragraphes qui suivent sont organisés de la façon suivante: après une première série d'exigences générales (permettant d'introduire les principaux concepts du SC, mais aussi le vocabulaire et la terminologie), nous consacrerons un tableau d'exigences par fonction du SC (13.2.2) (13.2.3), ces dernières précisant parfois certaines de celles qui les auront précédées. Pour terminer, quelques tableaux permettront d'exprimer des éléments qui n'auront pas eu leur place ailleurs.

La lecture de ces tableaux (tableaux 13.1 à 13.14, paragraphes 13.4.2 à 13.4.15) est un exercice fastidieux qui n'apporte pas grand-chose en soi à la compréhension de la démarche globale du travail; ils en constituent uniquement un des aboutissements concrets. C'est d'ailleurs pour cette raison, mais aussi parce qu'il y est fait quelques fois référence dans les derniers chapitres, qu'ils ont été maintenus dans ce document et non placés parmi les annexes; le lecteur pourra donc se contenter de les parcourir rapidement en diagonale, quitte à y revenir par la suite pour vérifier l'un ou l'autre point précis.

Conformément à notre habitude, chaque exigence sera identifiée par un code unique et fera référence au concept qu'elle implémente ou à l'exigence qu'elle complète.

[180] Le sujet *utilisateur* disposerait donc du droit de *création* sur l'objet de type *session*.

[181] Le lecteur objectera que suivant ce modèle, un employé *X* pourrait créer une session [G] en invitant le client *Y*, ensuite y inviter le client *Z* (notons que les deux invités, en qualité de clients différents, ne sont pas supposés avoir chacun connaissance de l'existence de l'autre (4.4.3.a)), puis quitter la session[G] en y laissant les deux clients (alors que le SC ne devrait pas permettre à des clients de converser entre eux (3.1.d)). Ceci toutefois ne pourra jamais conférer à *Y* ni à *Z* le droit ni la possibilité de s'inviter mutuellement par la suite; quant au choix de *X*, tenant compte du niveau de prise de conscience de la problématique de la sécurité (13.3.2.a), nous considérons a priori qu'il est responsable, motivé et défendable.

13.4.2. Définitions, terminologie et dispositions générales

Tableau 13.1	**Définitions, terminologie et dispositions générales**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.2.a)	Le projet consiste à mettre en place un système de communication vocale via l'Internet: le SC.	(2.2.b)
(13.4.2.b)	Le SC n'est pas public.	(3.1.c)
(13.4.2.c)	Le SC sera constitué d'un serveur et de plusieurs clients.	(5.2.4.1.a) (13.1.3.a)
(13.4.2.d)	Le *serveur du SC* sera une application informatique exécutée par une machine physiquement située au siège social de l'entreprise (sous-système *serveur* (13.1.3.a)).	(4.4.3.f) (5.2.4.1.b)
(13.4.2.e)	La machine qui exécutera le serveur du SC est nommée *serveur d'application du SC*.	
(13.4.2.f)	Les clients du SC seront des applications informatiques exécutées par des postes de travail individuels (sous-systèmes *local* et *distants* (13.1.3.a)).	
(13.4.2.g)	Tout poste de travail individuel qui exécutera un client du SC sera nommé *client d'application du SC*.	
(13.4.2.h)	Chaque client du SC devra pouvoir communiquer avec le serveur du SC par l'intermédiaire de réseaux non sécurisés.	
(13.4.2.i)	Les clients du SC ne communiqueront jamais directement entre eux; chaque communication impliquera un client du SC et le serveur du SC.	(4.6.6.a) (5.2.4.2.a)
(13.4.2.j)	Le SC n'est pas destiné à transporter autre chose que la voix.	
(13.4.2.k)	Le SC ne devra pas exploiter le mode IP *multicast*[G].	(13.1.4.a)
(13.4.2.l)	Le SC ne sera utilisable que par les individus qui y auront été préalablement enregistrés, c'est à dire dont l'identité lui sera connue.	(13.4.2.b)
(13.4.2.m)	Tout individu enregistré dans le SC est réputé *utilisateur* du SC.	
(13.4.2.n)	Le SC doit identifier et authentifier de façon unique les utilisateurs (13.4.2.m) (F_AUTH).	(6.4.5.i) (7.4.2.o) (8.3.2.a)
(13.4.2.o)	Un utilisateur (13.4.2.m) employé de l'entreprise sera nommé administrateur du SC.	
(13.4.2.p)	L'administrateur (13.4.2.o) du SC est responsable de l'enregistrement (enrôlement[G]: F_ENROL) des utilisateurs (13.4.2.m).	(4.4.3.g) (5.2.4.2.b) (7.4.2.w)
(13.4.2.q)	Les utilisateurs (13.4.2.m) ne pourront pas modifier eux-mêmes leurs données d'enregistrement (13.4.2.p).	(13.4.2.p)
(13.4.2.r)	Dans une seconde phase toutefois, et si les données d'enregistrement (13.4.2.p) des utilisateurs (13.4.2.m) contiennent un secret, ils devront pouvoir changer eux-mêmes ce secret.	(13.4.2.q)
(13.4.2.s)	Toute identification[G] et authentification[G] (13.4.2.n) réussies de l'utilisateur (13.4.2.m) auprès du SC établi une connexion[G] entre l'utilisateur (13.4.2.m) et le SC; l'utilisateur (13.4.2.m) est dit *connecté*.	(13.4.2.n)
(13.4.2.t)	Hormis l'identification[G] et l'authentification[G] (13.4.2.n), aucune interaction d'un utilisateur avec le SC n'est possible sans connexion[G] (13.4.2.s) de cet utilisateur au SC. Par la suite, chaque fois qu'il sera fait mention d'une interaction entre un utilisateur et le SC, cet utilisateur sera réputé connecté (13.4.2.s).	(4.5.3.f) (8.3.2.b)
(13.4.2.u)	Tout utilisateur accède automatiquement à la consultation du répertoire (F_REPER).	
(13.4.2.v)	La fonction du répertoire (F_REPER) a pour but de permettre à chaque utilisateur de choisir un correspondant parmi d'autres utilisateurs connectés (13.4.2.s).	
(13.4.2.w)	L'invitation[G] est la procédure par laquelle un utilisateur demande au SC de lui permettre d'entrer en communication vocale avec un autre utilisateur connecté (13.4.2.s) choisi dans son répertoire (F_INVIT).	
(13.4.2.x)	L'utilisateur (13.4.2.m) qui procède à une invitation[G] (13.4.2.w) est dit *invitant*.	
(13.4.2.y)	L'utilisateur (13.4.2.m) connecté (13.4.2.s) qui fait l'objet d'une invitation[G] (13.4.2.w) est dit *invité*.	
(13.4.2.z)	Si un utilisateur invité (13.4.2.y) accepte l'invitation[G] qui lui est faite, le SC établit une *session* [G] (F_SESS) permettant à l'utilisateur invitant et à l'utilisateur invité de converser ensemble (I_COMM).	

Tableau 13.1	**Définitions, terminologie et dispositions générales**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.2.aa)	Le SC doit pouvoir fonctionner en mode conférence, c'est-à-dire permettre des sessions [G] (13.4.2.z) impliquant plus de deux utilisateurs (13.4.2.m).	(3.1.e)
(13.4.2.ab)	Tout utilisateur qui participe à une session [G] (13.4.2.z) peut interrompre temporairement sa participation à cette session en rappelant la fonction du répertoire.	
(13.4.2.ac)	Tout utilisateur qui interrompt temporairement sa session [G] (13.4.2.z) en rappelant la fonction du répertoire est réputé *occupé hors session.*	(13.4.2.ab)
(13.4.2.ad)	Tout utilisateur qui participe de manière non interrompue à une session est réputé *occupé en session.*	(13.4.2.ab)
(13.4.2.ae)	Tout utilisateur occupé hors session (13.4.2.ac) peut inviter un autre utilisateur connecté (13.4.2.s) à se joindre à la session [G] (13.4.2.z) à laquelle il vient de suspendre sa participation.	
(13.4.2.af)	Tout utilisateur occupé hors session (13.4.2.ac) qui procède à une nouvelle invitation[G] devient *occupé en invitation.*	(13.4.2.ae)
(13.4.2.af)	Tout utilisateur occupé hors session (13.4.2.ac) qui ne procède pas à une nouvelle invitation[G] peut reprendre la session temporairement suspendue et revenir *occupé en session.*	(13.4.2.ae)
(13.4.2.ag)	Tout utilisateur invitant ou invité qui ne participe pas déjà à une session[G] est réputé *en invitation.*	
(13.4.2.ah)	Un utilisateur *occupé* est toujours *occupé en session* (13.4.2.ad), *occupé hors session* (13.4.2.ac) ou (exclusif) *occupé en invitation* (13.4.2.af).	
(13.4.2.ai)	Tout utilisateur connecté qui n'est ni occupé (13.4.2.ah) ni en invitation (13.4.2.ag) est réputé *disponible.*	
(13.4.2.aj)	Le statut d'un utilisateur connecté (13.4.2.s) indique si cet utilisateur est disponible (13.4.2.ai), en invitation, occupé (13.4.2.ah) hors session, occupé en session, ou occupé en invitation (13.4.2.ag).	
(13.4.2.ak)	Le statut (13.4.2.aj) d'un utilisateur connecté (13.4.2.s) ne pourra jamais être visible par un autre utilisateur connecté (13.4.2.s) sauf dans le cas où ils participent à la même session.	(4.4.3.b)
(13.4.2.al)	Le SC comptabilise un *canal de communication* par utilisateur participant à une session [G] (13.4.2.z).	(4.4.3.g) (4.4.3.h) (4.6.6.b)
(13.4.2.am)	Le SC comptabilise un *canal de communication distant* par utilisateur d'un sous-système *distant* (13.1.3.a) participant à une session [G] (13.4.2.z).	
(13.4.2.an)	Un utilisateur ne peut participer qu'à une seule session (13.4.2.z) à la fois.	
(13.4.2.ao)	Lorsqu'un utilisateur abandonne une session [G] (13.4.2.z), il redevient automatiquement disponible.	
(13.4.2.ap)	Toutes les communications entre clients et serveur du SC seront chiffrées sans exception aucune.	(4.5.3.g) (4.4.3.h) (4.4.3.i) (4.4.3.j) (7.4.2.t) (11.3.3.e) (11.6.b) (13.4.2.h)
(13.4.2.aq)	Une clé de chiffrement symétrique sera négociée avant chaque demande d'identification[G] et d'authentification[G]; en cas de connexion[G], cette clé sera utilisée pour chiffrer tous les flux liés à cette connexion[G].	(4.5.3.h)
(13.4.2.ar)	Toutes les données persistantes requises par le SC devront être conservées dans une base de données située sur le serveur d'application du SC (sous-système *serveur* (13.1.3.a)).	(4.4.3.e) (5.2.4.2.c) (7.4.2.b)
(13.4.2.as)	Le SC doit comporter un composant d'imputation destiné à permettre le suivi d'exploitation en termes de charge, de performances, de sécurité et d'incidents. Destinée à l'administrateur du SC, les informations générées ne peuvent en aucun cas être utilisées telles quelles pour retracer l'activité d'un utilisateur particulier.	(4.5.1.a) (7.4.2.o) (7.4.2.x)

Tableau 13.1	**Définitions, terminologie et dispositions générales**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.2.at)	Le SC doit comporter un composant de journalisation destiné à permettre la journalisation individuelle d'événements intéressant chaque utilisateur connecté (13.4.2.s). Destinées chaque fois à l'usage privé de l'unique utilisateur concerné, les informations générées ne peuvent en aucun cas être utilisées telles quelles pour retracer l'activité du SC globalement ou d'un autre utilisateur en particulier.	(4.5.1.a) (7.4.2.x)

13.4.3. Identification et authentification des utilisateurs: F_AUTH

Tableau 13.2	**Identification et authentification des utilisateurs**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.3.a)	L'identification[G] de l'utilisateur (13.4.2.m) requiert un login; l'authentification[G] de l'utilisateur (13.4.2.m) s'effectue grâce à un secret et via l'analyse de la signature biométrique (11.5) de sa frappe au clavier.	(4.5.3.f)
(13.4.3.b)	L'authentification[G] via le secret se fera selon le mode *challenge - response* (principe du protocole CHAP); le secret lui-même ne sera jamais transmis et le mot de passe transmis sera un OTP.	(4.5.3.h)
(13.4.3.c)	L'authentification[G] via la signature biométrique de la frappe au clavier de l'utilisateur se fera conformément à la méthode du prototype testé (11.5): la signature biométrique établie lors de l'authentification[G] sera transmise au serveur du SC qui la comparera à l'échantillon de référence de l'utilisateur dont l'identité aura été déclinée.	
(13.4.3.d)	L'authentification[G] via la signature biométrique de la frappe au clavier de l'utilisateur tiendra compte d'une valeur de seuil d'acceptation (distance relative) propre à l'utilisateur dont l'identité aura été déclinée ou, à défaut, d'une valeur de seuil d'acceptation (distance relative) commune à tous les utilisateurs du SC.	(11.5.2.1.a)
(13.4.3.e)	La procédure d'identification[G] et d'authentification[G] est réussie si l'utilisateur existe et si son mot de passe comme sa signature biométrique sont acceptés par le serveur du SC; il y a échec dans tous les autres cas.	
(13.4.3.f)	En cas d'échec (13.4.3.e) de l'identification[G] ou d'un des mécanismes d'authentification[G] d'un utilisateur, cet utilisateur sera invité à recommencer la procédure complète.	
(13.4.3.g)	En cas d'échec (13.4.3.e) de l'identification[G] ou d'un des mécanismes d'authentification[G] d'un utilisateur, aucune information sur la cause précise de l'échec (identité erronée, mot de passe erroné ou signature biométrique refusée) ne sera accessible à l'utilisateur concerné.	
(13.4.3.h)	La signature biométrique (13.4.3.a) pourra être établie sur base du login ou sur toute autre chaîne de caractères à l'exception du secret de l'utilisateur (13.4.2.m).	(13.4.2.q) (13.4.2.r)
(13.4.3.i)	Le SC ne permettra pas aux utilisateurs de sauvegarder localement de manière permanente leurs paramètres de connexion[G] (13.4.3.a), sous quelque forme que ce soit.	(4.4.3.e)
(13.4.3.j)	Le serveur du SC devra, à intervalles réguliers, soumettre chaque client du SC connecté à un nouveau challenge (principe renforcé du protocole CHAP); chaque client du SC devra être en mesure d'y répondre automatiquement sans intervention de l'utilisateur.	(11.3.3.c)
(13.4.3.k)	La *déconnexion* d'un utilisateur (13.4.2.m) connecté (13.4.2.s) au SC consiste à faire considérer par le SC que l'identification[G] (13.4.3.a) et l'authentification[G] (13.4.3.a) de l'utilisateur sont caduques; la connexion [G] de l'utilisateur (13.4.2.m) au SC est détruite.	(3.3.2.b)
(13.4.3.l)	Tout utilisateur (13.4.2.m) connecté (13.4.2.s) au SC doit pouvoir se déconnecter (13.4.3.k) du SC.	(3.3.2.b)
(13.4.3.m)	Un utilisateur (13.4.2.m) est réputé accessible par le SC quand il est connecté (13.4.2.s) au SC et que le SC est en mesure d'utiliser la connexion[G] établie avec cet utilisateur (13.4.2.m) pour prendre l'initiative de lui transmettre des informations.	
(13.4.3.n)	Tout utilisateur (13.4.2.m) connecté (13.4.2.s) au SC doit être accessible (13.4.3.m) par le SC.	

Tableau 13.2	**Identification et authentification des utilisateurs**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.3.o)	Aucun utilisateur (13.4.2.m) non connecté (13.4.2.s) au SC ne peut être accessible (13.4.3.m) par le SC.	(13.4.2.t)
(13.4.3.p)	Le SC devra vérifier régulièrement si les utilisateurs (13.4.2.m) connectés (13.4.2.s) sont accessibles (13.4.3.m).	
(13.4.3.q)	Le SC devra déconnecter (13.4.3.k) automatiquement tout utilisateur (13.4.2.m) connecté (13.4.2.s) qui ne serait plus accessible (13.4.3.m).	(3.3.2.b)
(13.4.3.r)	Dans une seconde phase, l'authentification[G] du serveur du SC auprès des clients qui souhaitent s'y connecter pourrait être envisagée. A l'exception de ce qui concerne la signature biométrique, cette authentification[G] devra alors obéir aux mêmes règles que celles édictées pour l'authentification[G] des clients auprès du serveur du SC (13.4.3.b) (13.4.3.e).	

13.4.4. Gestion du répertoire: F_REPER

Tableau 13.3	**Gestion du répertoire**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.4.a)	La fonction du répertoire (F_REPER) fournit à chaque utilisateur la liste des autres utilisateurs connectés auxquels il est autorisé à envoyer une invitation[G]; cette liste est appelée *contenu du répertoire*.	(3.1.d) (4.4.3.a) (13.4.2.v)
(13.4.4.b)	Le contenu du répertoire est individuel et peut être différent pour chaque utilisateur.	(13.4.4.a) (13.4.2.v)
(13.4.4.c)	Le contenu du répertoire comporte uniquement les informations relatives au profil des utilisateurs connectés.	(13.4.2.ak)
(13.4.4.d)	Le contenu du répertoire de chaque utilisateur est tenu à jour en temps réel par le SC au gré des connexions et déconnexions des utilisateurs.	(2.1.3.a) (13.4.2.v)
(13.4.4.e)	Un utilisateur ne pourra choisir de correspondant que parmi les utilisateurs qui figureront dans son répertoire.	(13.4.4.a) (13.4.2.v)
(13.4.4.f)	Le répertoire ne permettra d'inviter qu'un seul correspondant à la fois.	
(13.4.4.g)	La sélection du correspondant à inviter dans le répertoire pourra s'effectuer via des *radio buttons*.	(13.4.4.f)
(13.4.4.h)	Après sélection du correspondant dans le répertoire, un bouton de confirmation doit permettre à l'utilisateur de demander au SC de lancer l'invitation[G].	
(13.4.4.i)	Dès qu'il a demandé au SC de lancer son invitation[G], l'utilisateur est réputé invitant.	(13.4.2.x)
(13.4.4.j)	Le répertoire doit également offrir à l'utilisateur connecté une fenêtre lui permettant d'accéder au contenu de son journal personnel (13.4.2.at).	

13.4.5. Gestion des invitations: F_INVIT

Tableau 13.4	**Gestion des invitations**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.5.a)	L'invitation[G] (13.4.2.w) est une procédure qui implique un seul utilisateur invitant (13.4.2.x) et un seul utilisateur invité (13.4.2.y).	(13.4.4.f)
(13.4.5.b)	Lorsqu'il reçoit une demande de lancement (13.4.4.h) d'une invitation[G] (13.4.2.w), le serveur du SC marquera l'utilisateur à l'origine de la demande comme utilisateur invitant (13.4.2.x), puis vérifiera que le niveau courant des performances du réseau l'autorise à créer le ou les canaux de communication supplémentaire(s).	(4.3.3.h) (4.3.3.g) (4.6.6.c)

Tableau 13.4	**Gestion des invitations**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.5.c)	Si le niveau courant des performances du réseau n'autorise pas le serveur du SC à créer le ou les canaux de communication supplémentaire(s), la demande d'invitation[G] est annulée, l'annulation est motivée et l'utilisateur invitant (13.4.2.x) retrouve le statut qui était le sien avant l'introduction de sa demande d'invitation[G] (*disponible* ou *occupé hors session*[G]).	(13.4.5.b)
(13.4.5.d)	Si le niveau courant des performances du réseau autorise le serveur du SC à créer le ou les canaux de communication supplémentaire(s), le serveur du SC devra soumettre l'utilisateur invitant (13.4.2.x) à une nouvelle procédure d'identification et d'authentification[G].	(4.3.3.h) (4.3.3.g) (4.5.3.i) (4.5.3.j)
(13.4.5.e)	Si la nouvelle procédure d'identification[G] et d'authentification[G] de l'utilisateur invitant (13.4.2.x) échoue (13.4.3.e), la demande d'invitation[G] est annulée, l'annulation est motivée (13.4.3.g) et l'utilisateur invitant (13.4.2.x) retrouve le statut qui était le sien avant l'introduction de sa demande d'invitation[G] (*disponible* ou *occupé hors session*[G]).	(13.4.5.d)
(13.4.5.f)	Si la nouvelle procédure d'identification[G] et d'authentification[G] de l'utilisateur invitant réussit (13.4.3.e), la demande d'invitation[G] est acceptée et le serveur du SC marquera l'utilisateur faisant l'objet de l'invitation[G] comme étant invité (13.4.2.y).	
(13.4.5.g)	Un utilisateur invité qui n'était pas disponible au moment de l'acceptation par le serveur du SC de la demande d'invitation[G] (13.4.5.f) le visant sera dit *préalablement indisponible*.	
(13.4.5.h)	Un utilisateur invité qui était disponible au moment de l'acceptation par le serveur du SC de la demande d'invitation[G] (13.4.5.f) le visant sera dit *préalablement disponible*.	
(13.4.5.i)	Tout utilisateur invité (13.4.2.y) doit être averti de l'invitation[G] (13.4.2.w) et de son origine.	
(13.4.5.j)	Tout au long de la durée de l'invitation[G], la signification (13.4.5.i) de l'invitation[G] à un utilisateur invité préalablement disponible (13.4.5.h) doit être de type intermittent (sonnerie et/ou image animée); un retour d'information similaire mais non identique doit être fourni à l'invitant.	
(13.4.5.k)	La signification de l'invitation[G] à un utilisateur invité préalablement indisponible (13.4.5.g) doit être de type événementiel (une unique fenêtre pop-up du style JavaScript alert().	
(13.4.5.l)	Le retour d'information à l'invitant de la signification de l'invitation[G] à un utilisateur invité préalablement indisponible (13.4.5.k) sera identique à ce qu'il aurait été si l'utilisateur invité était préalablement disponible (13.4.5.h).	(13.4.2.ak)
(13.4.5.m)	Une invitation[G] expire automatiquement après un délai nommé *délai d'expiration de l'invitation*.	
(13.4.5.n)	Le délai d'expiration de l'invitation[G] est utilisé pour initialiser un *temporisateur* lors de l'acceptation par le SC de la demande d'invitation[G].	
(13.4.5.o)	Il y a demande de réponse à une invitation[G] (13.4.2.w) si l'utilisateur invité (13.4.2.y) signifie au SC endéans le délai d'expiration de l'invitation[G] (13.4.5.m) qu'il accepte d'entrer en session[G] (13.4.2.z) avec l'utilisateur invitant (13.4.2.z).	
(13.4.5.p)	Un utilisateur invité préalablement indisponible (13.4.5.g) ne peut introduire de demande de réponse (13.4.5.o) à une invitation[G] (13.4.2.w).	(13.4.2.an)
(13.4.5.q)	Lorsqu'il reçoit une demande de réponse (13.4.4.h) à une invitation[G], le SC devra soumettre l'utilisateur invité à une nouvelle procédure d'identification[G] et d'authentification[G].	(4.5.3.i) (4.5.3.j)
(13.4.5.r)	Si la nouvelle procédure d'identification[G] et d'authentification[G] de l'utilisateur invité échoue (13.4.3.e), sa demande de réponse à l'invitation[G] est annulée et le temporisateur (13.4.5.m) est réinitialisé à la valeur du délai d'expiration de l'invitation[G] (13.4.5.n).	
(13.4.5.s)	Si la nouvelle procédure d'identification[G] et d'authentification[G] de l'utilisateur invité (13.4.2.y) réussit, la demande de réponse de l'utilisateur invité est acceptée.	

Tableau 13.4	**Gestion des invitations**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.5.t)	Si la demande de réponse de l'utilisateur invité est acceptée (13.4.5.s) et si l'utilisateur invitant fait déjà partie d'une session[G], l'utilisateur invité rejoint la session [G] (13.4.2.z) de l'utilisateur invitant[182] et son statut devient *occupé en session*[G].	
(13.4.5.u)	Si la demande de réponse de l'utilisateur invité est acceptée (13.4.5.s) et si l'utilisateur invitant fait déjà partie d'une session[G], l'utilisateur invitant rejoint automatiquement sa session [G] (13.4.2.z) et son statut redevient *occupé en session*[G].	
(13.4.5.v)	Si la demande de réponse de l'utilisateur invité est acceptée (13.4.5.s) et si l'utilisateur invitant ne fait pas encore partie d'une session[G], le serveur du SC crée une nouvelle session[G] pour les deux utilisateurs; le statut des deux utilisateurs devient *occupé en session*[G].	
(13.4.5.w)	L'absence de réponse (13.4.5.o) à une invitation[G] (13.4.2.w) par l'utilisateur invité (13.4.2.y) ne pourra permettre à l'utilisateur invitant de déterminer si l'utilisateur invité est absent ou était préalablement indisponible (13.4.5.g).	(13.4.2.ak)
(13.4.5.x)	Si un utilisateur invité préalablement indisponible (13.4.5.g) redevient disponible avant la fin du délai d'expiration de l'invitation[G] (13.4.5.m), le serveur du SC reprendra la procédure d'invitation[G] comme si la demande d'invitation[G] venait d'être acceptée (13.4.5.f). et considèrera l'utilisateur invité comme préalablement disponible (13.4.5.h).	
(13.4.5.y)	A défaut de réponse (13.4.5.o) à l'invitation[G] (13.4.2.w) endéans le délai d'expiration de l'invitation[G] (13.4.5.m), l'invitation[G] se termine et l'utilisateur invitant (13.4.2.x) conserve le statut qui était le sien avant l'introduction de sa demande d'invitation[G] (*disponible* ou *occupé en session*[G]).	
(13.4.5.z)	A défaut de réponse (13.4.5.o) à l'invitation[G] (13.4.2.w) endéans le délai d'expiration de l'invitation[G] (13.4.5.m), l'invitation[G] se termine et la signification de l'invitation[G] à l'invité doit être de journalisée sous la forme d'un item dans le journal personnel de l'invité (13.4.2.at).	
(13.4.5.aa)	A défaut de réponse (13.4.5.o) à l'invitation[G] (13.4.2.w) endéans le délai d'expiration de l'invitation[G] (13.4.5.m), l'invitation[G] se termine et l'utilisateur invité (13.4.2.y) préalablement disponible (13.4.5.h) redevient disponible.	
(13.4.5.ab)	A défaut de réponse (13.4.5.o) à l'invitation[G] (13.4.2.w) endéans le délai d'expiration de l'invitation (13.4.5.m), l'invitation[G] se termine et l'utilisateur invité (13.4.2.y) préalablement indisponible (13.4.5.g) conserve son statut.	

13.4.6. Gestion des sessions: F_SESS

Tableau 13.5	**Gestion des sessions**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.6.a)	Tout utilisateur occupé en session[G] (13.4.2.ad) doit connaître à tout moment l'identité de tous les utilisateurs participant à la même session[G] (13.4.2.z).	(4.4.3.c)
(13.4.6.b)	Tous les utilisateurs participant à une même session[G] sont en mesure de converser entre eux.	
(13.4.6.c)	Lorsque le matériel le supporte, les conversations (13.4.6.b) devront être possibles en duplex intégral.	
(13.4.6.d)	Un utilisateur occupé en session[G] (13.4.2.ad) doit pouvoir quitter la session[G] (13.4.2.z) à tout moment par simple action sur un bouton.	
(13.4.6.e)	Un utilisateur occupé en session[G] (13.4.2.ad) qui quitte (13.4.6.d) une session[G] (13.4.2.z) est automatiquement renvoyé à la consultation de son répertoire (13.4.4.c) (13.3.4.a) et redevient disponible (13.4.2.ai).	

[182] Signalons qu'en pratique, certains protocoles de signalisation créent une nouvelle session, y placent le dernier venu et réémettent de nouvelles invitations pour transférer automatiquement les autres utilisateurs vers la nouvelle session avant de clôturer l'ancienne. Mais du point de vue fonctionnel, tout semble se passer comme nous l'avons écrit (le nouvel utilisateur semble être simplement ajouté à la session en cours).

Tableau 13.5	**Gestion des sessions**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.6.f)	Un utilisateur occupé en session[G] (13.4.2.ad) doit pouvoir suspendre temporairement la session[G] (13.4.2.z) à tout moment par simple action sur un bouton.	
(13.4.6.g)	Un utilisateur occupé en session[G] (13.4.2.ad) qui suspend temporairement (13.4.6.f) une session[G] (13.4.2.z) est automatiquement renvoyé à la consultation de son répertoire (13.4.4.c) (13.3.4.a) et devient occupé hors session[G].	
(13.4.6.h)	Il y a *inactivité* pour un utilisateur occupé en session[G] (13.4.2.ad) lorsque cet utilisateur n'émet ni ne reçoit rien. Une durée maximum d'inactivité doit pouvoir être paramétrée.	
(13.4.6.i)	Lorsqu'un utilisateur occupé en session[G] (13.4.2.ad) s'est trouvé inactif pendant un laps de temps supérieur à la durée maximale d'inactivité (13.4.6.h), celui-ci quitte automatiquement la session[G] en cours.	
(13.4.6.j)	Lorsqu'une session[G] (13.4.2.z) ne comporte plus qu'un seul utilisateur occupé en session[G] (13.4.2.ad), celui-ci la quitte automatiquement.	
(13.4.6.k)	Une session[G] (13.4.2.z) se termine quand elle ne compte plus d'utilisateur occupé en session[G] (13.4.2.ad).	
(13.4.6.l)	Tous les échanges effectués dans le cadre d'une session[G] empruntent les connexions[G] des utilisateurs occupés en session[G] (13.4.2.ad) dans cette session[G] [183].	

13.4.7. Imputation et journalisation: F_AUDIT

Tableau 13.6	**Imputation et journalisation**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.7.a)	Le composant d'imputation (13.4.2.as) doit être capable d'enregistrer toutes les demandes d'identification[G] et d'authentification[G] avec les informations suivantes: date, heure, identificateur unique de l'événement, statut de la demande (succès ou échec), identité déclarée par l'utilisateur (en cas d'échec seulement), adresse IP de l'origine de la demande (en cas d'échec seulement), nombre d'utilisateurs connectés, de sessions[G] ouvertes, de canaux (13.4.2.al) ouverts et de canaux distants (13.4.2.am) ouverts consécutivement à la demande, évaluation (forme à déterminer) des performances courantes du réseau.	(4.5.3.m) (8.3.2.m) (13.4.2.as)
(13.4.7.b)	Le composant d'imputation (13.4.2.as) doit être capable d'enregistrer toutes les invitations[G] effectuées par les utilisateurs avec les informations suivantes: date, heure, identificateur unique de l'événement, statut de la demande (succès ou échec), en cas d'échec la cause de l'échec (absence de réponse, utilisateur invité occupé, limites du SC atteintes), nombre d'utilisateurs connectés, de sessions[G] ouvertes, de canaux (13.4.2.al) ouverts et de canaux distants (13.4.2.am) ouverts consécutivement à la demande, évaluation (forme à déterminer) des performances courantes du réseau.	(8.3.2.n) (13.4.2.as)
(13.4.7.c)	Le composant d'imputation (13.4.2.as) doit être capable d'enregistrer tous les abandons (13.4.6.d) de session des utilisateurs avec les informations suivantes: date, heure, identificateur unique de l'événement, nombre d'utilisateurs connectés, de sessions[G] ouvertes, de canaux (13.4.2.al) ouverts et de canaux distants (13.4.2.am) ouverts consécutivement à la demande, évaluation (forme à déterminer) des performances courantes du réseau.	(8.3.2.o) (13.4.2.as)

[183] Tenant compte du fait que la clé de chiffrement symétrique est propre à chaque connexion, et que tous les flux (y compris le contenu des conversations: I_COMM) transitent par le serveur du SC, il y aura donc déchiffrement puis chiffrement à nouveau du contenu des conversations au passage du serveur du SC.

Tableau 13.6	**Imputation et journalisation**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.7.d)	Le composant d'imputation (13.4.2.as) doit être capable d'enregistrer toutes les demandes de déconnexion des utilisateurs avec les informations suivantes: date, heure, identificateur unique de l'événement, origine de la demande (déconnexion volontaire (13.4.3.l) ou forcée (13.4.3.q)), nombre d'utilisateurs connectés, de sessions[G] ouvertes, de canaux (13.4.2.al) ouverts et de canaux distants (13.4.2.am) ouverts consécutivement à la demande, évaluation (forme à déterminer) des performances courantes du réseau.	(8.3.2.m) (13.4.2.as)
(13.4.7.e)	Seul l'administrateur du SC dispose d'un accès aux données enregistrées par le composant d'imputation (13.4.2.as).	(4.5.3.l) (7.4.2.w) (8.3.2.p)
(13.4.7.f)	Il doit exister des outils pour examiner et maintenir les fichiers d'imputation, et ces outils doivent être documentés.	(8.3.2.q)
(13.4.7.g)	Les outils d'analyse des fichiers d'imputation doivent permettre d'y effectuer des recherches sélectives	(8.3.2.r)
(13.4.7.h)	Le nombre et la nature des événements enregistrés par le composant d'imputation du serveur du SC doivent pouvoir évoluer facilement.	
(13.4.7.i)	Les données enregistrées par le composant d'imputation (13.4.2.as) constituent des données persistantes du SC.	(4.4.3.e)
(13.4.7.j)	Le composant de journalisation (13.4.2.at) doit être capable, pour chaque utilisateur, d'enregistrer toutes les invitations[G] auxquelles il n'a pas répondu avec les informations suivantes: date, heure, identificateur unique de l'événement et identité de l'utilisateur invitant.	(13.4.2.at)
(13.4.7.k)	Chaque item du journal personnel d'un utilisateur (13.4.2.at) doit lui être présenté accompagné d'un bouton EFFACER; l'utilisation de ce bouton provoquera l'effacement définitif de l'item.	
(13.4.7.l)	Chaque journal personnel d'un utilisateur (13.4.2.at) doit comporter un bouton EFFACER TOUS LES ITEMS: l'utilisation de ce bouton provoquera l'effacement définitif de tous les items de son journal.	(4.5.3.l)
(13.4.7.m)	Le nombre et la nature des événements journalisés dans le journal personnel de chaque utilisateur (13.4.2.at) doivent pouvoir évoluer facilement.	
(13.4.7.n)	Les données enregistrées par le composant de journalisation (13.4.2.at) du serveur du SC constituent des données persistantes du SC.	(4.4.3.e)
(13.4.7.o)	Les données enregistrées par le composant de journalisation (13.4.2.at) ne seront accessibles que de l'utilisateur concerné.	(4.5.3.l) (7.4.2.w)
(13.4.7.p)	Chaque utilisateur devra être en mesure de fournir au SC un secret sur base duquel le serveur du SC chiffrera les événements le concernant qui seront enregistrés par le composant de journalisation (13.4.2.at) du serveur du SC. Si nécessaire, toute modification de ce secret pourra être subordonnée au vidage préalable complet du journal personnel de l'utilisateur concerné.	(4.5.3.l) (13.4.7.o)
(13.4.7.q)	Une reconstitution de l'activité d'un utilisateur et son croisement avec l'activité du SC ne seront possibles qu'en croisant les données enregistrées par le composant de journalisation pour cet utilisateur avec celles enregistrées par le composant d'imputation.	(4.5.3.l)
(13.4.7.r)	Le SC et/ou le système d'exploitation du serveur d'application dédicacé au SC sont responsables de la rotation des fichiers d'imputation et de journalisation générés par le SC; le système d'exploitation est responsable de la conservation pour une durée déterminée, y compris de la sauvegarde sur un medium amovible, des fichiers d'imputation et de journalisation générés par le SC.	(7.4.2.w)

13.4.8. Gestion des utilisateurs: F_ENROL

Tableau 13.7	**Gestion des utilisateurs**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.8.a)	Hormis l'administrateur du SC, aucun individu ne pourra s'enregistrer lui-même dans le SC.	(13.4.2.p)
(13.4.8.b)	Les utilisateurs (13.4.2.m) seront identifiés individuellement et répartis en groupes d'utilisateurs (13.4.2.m). Chaque utilisateur (13.4.2.m) appartiendra à un et un seul groupe d'utilisateurs (13.4.2.m).	(8.3.2.d)
(13.4.8.c)	L'administrateur du SC est responsable de la répartition des utilisateurs en groupes d'utilisateurs.	(7.4.2.w)
(13.4.8.d)	Le profil (I_PROFIL (5.2.3.3.f)) de chaque utilisateur (13.4.2.m) devra inclure au minimum un identifiant, son nom, son prénom, ses numéros de téléphone et de fax, son e-mail, l'adresse de son lieu de travail habituel, son groupe (13.4.8.b) ainsi que les nom, adresse, numéros de téléphone et de fax de l'entreprise qui l'emploie.	
(13.4.8.e)	Les paramètres de connexion[G] (I_AUTH (5.2.3.3.e)) de chaque utilisateur (13.4.2.m) incluent son login, son mot de passe et sa signature biométrique.	(4.5.3.f)
(13.4.8.f)	Les paramètres de connexion[G] (I_AUTH (5.2.3.3.e)) de chaque utilisateur (13.4.2.m) pourront également inclure le seuil d'acceptation de sa signature biométrique, exprimé en termes de distance relative par rapport à son échantillon de référence conformément et selon la méthode du prototype testé.	(11.5.2.1.a) (13.4.3.d)
(13.4.8.g)	Les profils (13.4.8.d) et paramètres de connexion[G] (13.4.8.e) des utilisateurs (13.4.2.m) sont des informations requises pour l'enrôlement[G] des utilisateurs par l'administrateur (13.4.2.o) du SC.	(13.4.2.p)
(13.4.8.h)	Les profils (13.4.8.d) et paramètres de connexion[G] (13.4.8.e) des utilisateurs (13.4.2.m) sont des données persistantes du SC (13.4.2.ar).	(4.4.3.e)
(13.4.8.i)	Le SC ne comprendra pas de module de gestion des utilisateurs (13.4.2.m); l'administrateur (13.4.2.o) gèrera les profils (13.4.8.d) et paramètres de connexion[G] (13.4.8.e) des utilisateurs (13.4.2.m) par accès direct à la base de données utilisée par le SC.	(4.4.3.g) (5.2.4.2.b)
(13.4.8.j)	L'administrateur est garant de la qualité (longueur, prédictabilité) des mots de passe des utilisateurs (13.4.2.m).	
(13.4.8.k)	Dans une seconde phase, le SC devra être à même de vérifier la qualité (longueur, prédictabilité) des mots de passe modifiés par les utilisateurs (13.4.2.m) et d'associer à chaque mot de passe une durée limite de validité.	(13.4.2.q)
(13.4.8.l)	Le nombre et la nature des informations liées au profil (13.4.8.d) des utilisateurs du SC doivent pouvoir évoluer facilement.	

13.4.9. Configuration et administration: F_ADM

Tableau 13.8	**Configuration et administration**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.9.a)	Les informations de configuration comprennent les droits d'invitation[G] des utilisateurs et les paramètres du SC (F_PARAM).	
(13.4.9.b)	Les informations de configuration sont des données persistantes du SC (13.4.2.ar).	(4.4.3.e)
(13.4.9.c)	L'administrateur du SC est responsable de la configuration dans le SC des informations de configuration du SC.	(7.4.2.w)
(13.4.9.d)	Les paramètres du SC comprennent le délai d'expiration de l'invitation[G] (13.4.5.m).	(13.4.5.o)
(13.4.9.e)	Les paramètres du SC comprennent la durée maximale d'inactivité (13.4.6.h).	
(13.4.9.f)	Les paramètres du SC comprennent la valeur par défaut du seuil d'acceptation de la signature biométrique des utilisateurs, exprimé en termes de distance relative par rapport à un échantillon de référence conformément et selon la méthode du prototype testé.	(13.4.8.f) (11.5.2.1.a)

Tableau 13.8	**Configuration et administration**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.9.g)	Les paramètres du SC comprennent la durée maximale de connexion[G] qui peut s'écouler pour chaque utilisateur avant que le serveur du SC n'envoie un nouveau challenge au logiciel client.	(13.4.3.j)
(13.4.9.h)	Les paramètres du SC comprennent toutes informations nécessaires au SC pour apprécier les performances du réseau, et les valeurs pivot en deçà desquelles il refusera d'ouvrir un nouveau canal de communication (13.4.2.al) (nature de ces informations à déterminer).	(4.3.3.h) (4.6.6.c)
(13.4.9.i)	Les paramètres du SC comprennent le nombre maximum de canaux de communication distants ouverts que le SC peut gérer simultanément.	(4.3.3.g) (4.6.6.b)
(13.4.9.j)	Le SC ne devra pas comprendre de module d'administration; l'administrateur (13.4.2.o) gèrera les informations de configuration par accès direct à la base de données utilisée par le SC.	(4.4.3.d)
(13.4.9.k)	Le nombre et la nature des informations de configuration du SC doivent pouvoir évoluer facilement.	
(13.4.9.l)	Dans une seconde phase, les paramètres du SC comprendront également la durée limite de validité des mots de passe des utilisateurs.	(13.4.8.k)

13.4.10. Gestion des droits d'accès: F_ACTRL

Tableau 13.9	**Gestion des droits d'accès**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.10.a)	L'administrateur (13.4.2.o) du SC dispose seul d'un accès total (création, modification, suppression) aux données persistantes (13.4.8.h) (13.4.9.b) conservées dans la base de données située sur le serveur d'application du SC (sous-système *serveur* (13.1.3.a)).	(4.4.3.g) (6.4.5.k) (8.3.2.j)
(13.4.10.b)	Le SC dispose d'un accès en lecture aux données persistantes (13.4.8.h) (13.4.9.b) conservées dans la base de données située sur le serveur d'application du SC (sous-système *serveur* (13.1.3.a)).	(13.4.10.a)
(13.4.10.c)	Aucun autre sujet ne peut accéder aux données persistantes (13.4.8.h) (13.4.9.b) conservées dans la base de données située sur le serveur d'application du SC (sous-système *serveur* (13.1.3.a)).	(13.4.10.a)
(13.4.10.d)	La base de données exploitée par le SC et le système d'exploitation du serveur de l'application sont responsables des disponibilité, intégrité et confidentialité des données persistantes (13.4.8.h) (13.4.9.b) qui y sont conservées conformément à la politique de sécurité en vigueur (13.4.10.a) (13.4.10.b) (13.4.10.c) (13.4.8.j)	(7.4.2.w) (8.3.2.k) (8.3.2.l) (13.4.10.a)
(13.4.10.e)	L'administrateur (13.4.2.o) est responsable de la validité et de la confidentialité des profils (13.4.8.d) et paramètres de connexion[G] (13.4.8.e) des utilisateurs (13.4.2.m) lors de leur collecte et de l'enrôlement[G].	(4.5.3.k) (6.4.5.j) (7.4.2.w)
(13.4.10.f)	Les droits d'invitation[G] sont de deux ordres: génériques et contextuels.	
(13.4.10.g)	Par défaut, un utilisateur ne dispose d'aucun droit d'invitation[G]	(13.4.9.c)
(13.4.10.h)	Chaque droit d'invitation[G] générique concerne le droit d'un utilisateur sujet (invitant potentiel) à visualiser un utilisateur objet (invité potentiel) dans son répertoire.	
(13.4.10.i)	Les droits d'invitation[G] contextuels précisent les limites dans lesquelles un utilisateur sujet peut effectivement inviter un utilisateur objet choisi dans son répertoire.	
(13.4.10.j)	Le droit d'utiliser le dernier canal de communication (13.4.2.al) disponible du SC est un droit d'invitation[G] contextuel.	(4.3.3.d)
(13.4.10.k)	La détermination par le SC d'un droit d'invitation[G] contextuel d'un utilisateur *u1* (l'invitant) s'effectue selon la séquence suivante: - recherche sur base de l'identité de *u1*; si aucune réponse quant au droit n'est trouvée, alors - recherche sur base du groupe de *u1;* si aucune réponse quant au droit n'est trouvée, alors la valeur par défaut est appliquée.	

Tableau 13.9	**Gestion des droits d'accès**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.10.l)	Le nombre et la nature des droits d'invitation[G] contextuels doivent pouvoir évoluer facilement.	
(13.4.10.m)	Chaque droit d'invitation[G] générique doit pouvoir être établi sur base de l'identité des deux utilisateurs, sur base du groupe auquel un des deux utilisateurs appartient et de l'identité de l'autre utilisateur, ou sur base du groupe auquel chacun des deux utilisateurs appartient.	(8.3.2.d)
(13.4.10.n)	La détermination par le SC des droits d'invitation[G] génériques (13.4.10.h) d'un utilisateur *u2* (l'invité) par un utilisateur *u1* (l'invitant) s'effectue selon la séquence suivante: - recherche sur base de l'identité de *u1* et de l'identité de *u2*; si aucune réponse quant au droit n'est trouvée, alors - recherche sur base de l'identité de *u1* et du groupe de *u2*; si aucune réponse quant au droit n'est trouvée, alors - recherche sur base du groupe de *u1* et de l'identité de *u2*; si aucune réponse quant au droit n'est trouvée, alors - recherche sur base du groupe de *u1* et du groupe de *u2;* si aucune réponse quant au droit n'est trouvée, alors la valeur par défaut est appliquée.	(13.4.10.m)

13.4.11. Développement: F_DEVEL

Tableau 13.10	**Développement**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.11.a)	Le développement du SC devra s'effectuer dans un environnement sécurisé.	(4.7.3.e) (7.4.2.aa)
(13.4.11.b)	Le développement du SC devra s'effectuer selon une méthodologie et à l'aide d'outils définis préalablement et documentés.	(6.4.5.d)
(13.4.11.c)	La méthodologie de développement (13.4.11.b) inclut la définition du modèle de cycle de vie du produit.	(6.4.5.d)
(13.4.11.d)	Chaque fois que cela s'avérera relevant, le code source devra contenir en commentaire des références explicites aux exigences énoncées dans ce chapitre.	
(13.4.11.e)	L'analyse des risques doit reposer sur une approche formelle reconnue.	(7.4.2.p)
(13.4.11.f)	Les logiciels développés doivent faire l'objet d'une recette rigoureuse; les logiciels acquis doivent être isolés pour analyse avant d'être distribués.	(7.4.2.t)
(13.4.11.g)	Le SC devra être conçu et développé en respectant un corpus de règles ergonomiques (à définir).	(6.4.5.c)

13.4.12. Déploiement: F_DEPLO

Tableau 13.11	**Déploiement**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.12.a)	L'administrateur du SC est responsable du déploiement du SC.	(5.2.4.2.e) (7.4.2.w)
(13.4.12.b)	Le serveur du SC devrait pouvoir être déployé et mis en exploitation sans qu'il soit besoin de modifier la configuration des dispositifs de protection logique du siège central de l'entreprise.	
(13.4.12.c)	Le déploiement de la partie client du SC sur les différents types de clients répartis dans les sous-systèmes *local* et *distants* (13.1.3.a) devra être le plus automatisé possible.	
(13.4.12.d)	Le SC devra pouvoir être déployé et mis en exploitation au niveau des postes clients sans qu'il soit besoin de modifier la configuration des différents dispositifs de protection logique.	

Tableau 13.11	**Déploiement**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.12.e)	Le code source ne sera pas déployé.	(4.7.3.a) (5.2.4.2.d) (7.4.2.aa)

13.4.13. Maintenance: F_MAINT

Tableau 13.12	**Maintenance**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.13.a)	Toutes les anomalies de fonctionnement constatées au niveau du serveur d'application dédicacé au SC devront être journalisées.	(7.4.2.u)
(13.4.13.b)	Toutes les opérations de maintenance matérielle ou logicielle du serveur d'application dédicacé au SC devront être journalisées.	(7.4.2.u)
(13.4.13.c)	Chaque fois qu'une relation pourra être établie, dans un sens ou dans l'autre, entre une ou plusieurs anomalies de fonctionnement du serveur d'application dédicacé au SC et/ou une ou plusieurs opérations de maintenance matérielle et logicielle dudit serveur, cette relation devra être journalisée.	(13.4.13.a) (13.4.13.b)
(13.4.13.d)	L'administrateur du SC est responsable de la maintenance matérielle et logicielle du serveur d'application dédicacé au SC.	(7.4.2.w)
(13.4.13.e)	Toutes les anomalies de fonctionnement constatées au niveau du SC devront être journalisées.	(7.4.2.u)
(13.4.13.f)	Toutes les opérations de maintenance logicielle du SC devront être journalisées.	(7.4.2.u)
(13.4.13.g)	Chaque fois qu'une relation pourra être établie, dans un sens ou dans l'autre, entre une ou plusieurs anomalies de fonctionnement du SC et/ou une ou plusieurs opérations de maintenance logicielle du SC, cette relation devra être journalisée.	(13.4.13.e) (13.4.13.f)
(13.4.13.h)	L'administrateur du SC est responsable de la maintenance logicielle du SC.	(7.4.2.w)

13.4.14. Exigences techniques complémentaires

Tableau 13.13	**Exigences techniques complémentaires**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.14.a)	Tout utilisateur (13.4.2.m) disposant d'un poste de travail et d'une connexion à l'Internet devra être en mesure de se connecter (13.4.2.s) au SC quel que soit son lieu de travail.	(4.3.3.e)
(13.4.14.b)	Tout utilisateur (13.4.2.m) disposant d'un poste de travail et d'une connexion à l'Internet devra être en mesure de se connecter (13.4.2.s) au SC quels que soient le type et les caractéristiques matérielles et logicielles de son poste de travail.	(4.3.3.e)
(13.4.14.c)	Tout utilisateur (13.4.2.m) disposant d'un poste de travail et d'une connexion à l'Internet devra être en mesure de se connecter (13.4.2.s) au SC quels que soient son mode de connexion à l'Internet et les caractéristiques des dispositifs de protection logique locaux.	(4.3.3.e) (4.6.6.a)
(13.4.14.d)	Si le serveur d'application dédicacé au SC devait être situé en zone publique (DMZ), le système d'exploitation utilisé devra être conforme à la politique de l'entreprise concernant les type et configuration des systèmes d'exploitation habilités en zone publique.	(13.4.2.d)
(13.4.14.e)	La politique de l'entreprise concernant les type et configuration des systèmes d'exploitation habilités en zone publique étant évolutive par essence, un effort particulier au niveau de la portabilité du serveur du SC devra être consenti .	
(13.4.14.f)	La base de données utilisée par le SC ne supportera aucune connexion réseau de quelque nature que ce soit.	(4.4.3.d)
(13.4.14.g)	Le SC devra être portable pour supporter la disparité des environnements technologiques de l'entreprise.	

Tableau 13.13	**Exigences techniques complémentaires**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.14.h)	Le serveur du SC devra pouvoir fonctionner sur un serveur d'application du SC (13.4.2.e) qui serait une machine de récupération, typiquement un poste de travail ou serveur déclassé de type PC.	
(13.4.14.i)	Le SC devra pouvoir être mis en service sans imposer de modification de configuration (4.6.4.a) des dispositifs de protection logique de l'entreprise (4.6.3.a) (4.6.5.b).	(4.6.6.a)

13.4.15. Exigences non techniques complémentaires

Tableau 13.14	**Exigences non techniques complémentaires**	
Identifiant	*Exigences*	*Implémente ou complète*
(13.4.15.b)	Le projet devra être mené à terme sans qu'il soit besoin d'acquérir de logiciel ou de licence de logiciel.	
(13.4.15.c)	Le projet devra être mené à terme sans qu'il soit besoin d'acquérir de matériel autre que, le cas échéant, les matériels de capture et de restitution du son pour les différents clients d'application du SC (carte son, enceintes et micro).	
(13.4.15.d)	Une documentation technique du SC doit exister, et être suffisamment détaillée - voire procédurale - pour permettre à tout employé présent au siège central de l'entreprise d'intervenir rapidement en cas d'incident technique ou de sécurité.	(4.3.3.b) (7.4.2.q) (7.4.2.t)
(13.4.15.e)	La documentation technique et les procédures doivent être régulièrement diffusées, mises à jour et sauvegardées.	(7.4.2.q) (7.4.2.y) (13.4.15.d)
(13.4.15.f)	L'entreprise veillera à établir et faire respecter un tour de rôle garantissant tout au long de chaque journée de support la connexion[G] permanente d'au moins un employé au SC affecté prioritairement au support.	(4.3.3.c)
(13.4.15.g)	L'employé affecté prioritairement au support (13.4.15.f) veillera à être le plus souvent possible disponible.	(4.3.3.d)
(13.4.15.h)	Il devra être procédé à intervalles réguliers à des tests d'intrusion et à une réévaluation des procédures et configuration de sécurité.	(7.4.2.r)
(13.4.15.i)	Une documentation utilisateur du SC doit exister, et permettre d'assurer la guidance de l'utilisateur comme sa prise de conscience de la problématique de la sécurité.	(6.4.5.b) (6.4.5.f)
(13.4.15.j)	L'administrateur du SC devra assurer la formation des utilisateurs sur base du contenu et des objectifs de la documentation utilisateur (13.4.5.i).	(6.4.5.a) (6.4.5.f) (6.4.5.h)

13.5. Diagramme

13.5.1. Diagramme d'états de l'utilisateur

Le diagramme d'états de l'utilisateur qui découle des exigences est illustré par la figure 13.1 ci-dessous.

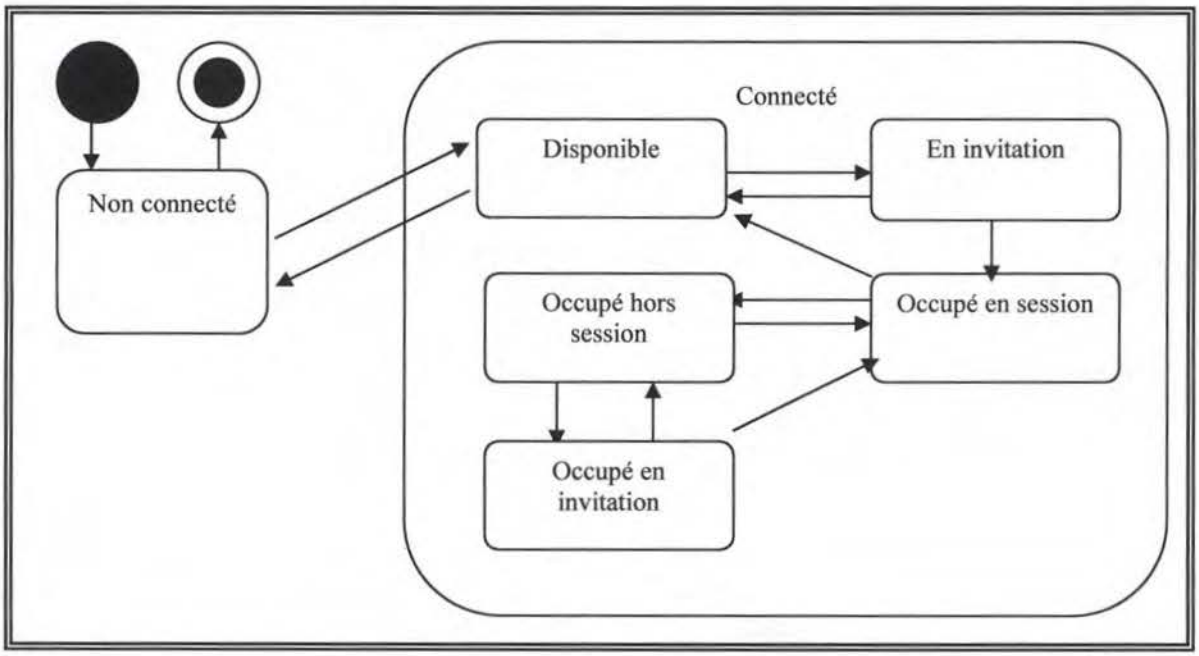


Figure 13.1: états de l'utilisateur enrôlé

Chapitre 14 Architecture

Dans ce chapitre, nous tentons d'esquisser les contours d'une architecture qui devrait être de nature à satisfaire les exigences énoncées au chapitre précédent.

14.1. Avertissement

La recherche d'architecture qui fait l'objet de ce chapitre constitue davantage la première pierre d'une démarche de réflexion qu'un point de départ pour développement. La plupart des options avancées ici sont de pures prospectives théoriques; faute de temps et de connaissances techniques suffisamment pointues des technologies envisagées, leur faisabilité n'a pas toujours été validée.

14.2. Proposition d'architecture

14.2.1. Hypothèses de travail

La proposition d'architecture qui suit est basée sur les hypothèses de travail suivantes:

- le transport de la voix via TCP représente un handicap acceptable. Cette hypothèse s'appuie sur les résultats de notre essai d'application du chapitre 10 (10.5) ainsi que sur l'existence sur le marché de produits au fonctionnement similaire;
- la faisabilité technique est réelle;

14.2.2. Présentation générale de l'architecture

La direction dans laquelle nous nous orienterions de prime abord est celle de l'application web traditionnelle à trois niveaux qui seraient:

- un client mince, le traditionnel navigateur web,
- un serveur d'application (serveur HTTP et serveur du SC) et
- la base de données du SC.

Toutes les communications entre clients et serveur s'effectueraient via le port 443 (SSL/TLS), ce qui garantirait à la fois le respect de nos exigences de chiffrement intégral, de négociation d'une clé symétrique et de respect de la configuration des dispositifs de protection logique.

14.2.3. Langage et technologie

L'ensemble de l'application (serveur et client du SC) serait écrit en java, ce qui devrait satisfaire nos exigences de portabilité du serveur, de versatilité du client (mince) ainsi que celle concernant l'automatisation du déploiement des modules clients (sous forme d'applets).

Tenant compte de la politique actuelle de l'entreprise, le serveur du SC serait à déployer en DMZ sur une machine à architecture PC configurée avec Linux[184], Apache[185] et Jakarta-tomcat[186].

14.2.4. Le client

Le client type serait un navigateur capable d'exécuter des applets java. Les communications entre le client et le serveur du SC se feraient toutes via le port 443 (SSL/TLS), que la plupart des infrastructures de protection logique permettent d'utiliser librement ou par l'intermédiaire d'un serveur proxy.

[184] Système d'exploitation open source (http://www.linux.org).
[185] Serveur HTTP open source (http://www.apache.org).
[186] Serveur JSP et servlets open source (http://jakarta.apache.org)

La partie client du SC, exécutée dans le navigateur, s'articulerait autour de 3 fonctions que nous envisageons sous la forme de trois applets distinctes mais capables de communiquer entre elles:

- une applet pour la fonction d'identification[G] et d'authentification[G] (F_AUTH),
- une applet pour les fonctions de gestion du répertoire (F_REPER) et d'invitation[G] (F_INVIT), et
- une applet pour gérer la connexion[G] et les sessions[G] (F_SESS).

Pour établir la connexion[G], l'utilisateur naviguerait vers une URL comme https://mysc.mycompany.com, où après le traditionnel handshake SSL (négociation des options et de la clé de chiffrement symétrique (12.6.1)) l'utilisateur téléchargerait et exécuterait une applet d'identification[G] et d'authentification[G] contenant un *challenge*. Cette applet permettrait la saisie locale du login, du secret et de la signature biométrique, convertirait le secret en mot de passe sur base du challenge et renverrait le tout chiffré par SSL au serveur du SC.

Une fois l'identification[G] et l'authentification[G] réussies, la connexion[G] (13.4.2.s) est établie et l'applet de gestion du répertoire et son contenu seraient téléchargés, ainsi que l'applet de gestion des sessions[G]. Cette dernière, de loin la plus complexe, devrait pouvoir prendre en charge:

- la matérialisation de la session[G], par exemple sous la forme d'un flux distinct (mais toujours sous SLL) entre le client et le serveur du SC (une servlet à une URL comme https://mysc.mycompany.com/scvpn);
- la saisie et la restitution de la parole;
- l'envoi et la réception de flux RTP/RTCP via le flux de session[G] établi.

La connexion[G] (13.4.2.s) et la session[G] seraient dès lors matérialisées, au niveau du serveur, par autant d'instanciations des classes correspondantes (*clientConnection* pour la première et *clientSession* pour la seconde), charge au serveur de gérer lui-même le routage des flux entre ces différentes instances. Mais la mécanique qui consisterait à générer puis envoyer un flux RTP via une communication applet-servlet (et inversement), pour peu qu'elle soit réalisable, ne risque pas d'être très simple à mettre au point.

14.2.5. Le serveur

Le serveur du SC devra principalement prendre en charge, outre les fonctions assez simples d'identification[G] et d'authentification[G] ou encore la mise à disposition des applets, toute la logistique du routage des flux de chaque session[G] vers les différents canaux de communication concernés. Fonctionnellement, il s'agit là du travail d'un translator (10.2.6), et toute la difficulté consistera à en implémenter ou incorporer un au sein du serveur du SC.

14.2.6. La signalisation

La signalisation est réduite à sa plus simple expression, puisque aucune des fonctions avancées qu'un protocole comme SIP (10.4.2) peut offrir n'est nécessaire ici. Dans notre cas, le serveur de notre SC sait pertinemment bien où et comment trouver chacun des utilisateurs (puisque seuls les utilisateurs connectés sont pris en considération), connaît probablement la plupart de leurs caractéristiques (puisqu'il s'agit d'une application homogène), et les problèmes de sécurité (10.4.3) ont été évacués vers SSL/TLS. Les besoins de signalisation qui restent (principalement les invitations[G], ainsi que les ouvertures et fermeture de sessions[G]) seront pris en charge par le SC.

14.2.7. La base de données

La base de données pourra être composée de fichiers plats, gérés et maintenus par l'administrateur à l'aide d'un simple éditeur de texte comme *vi*. L'organisation interne des informations (le contenu des fichiers) pourra être de type stanza (format des fichiers *.ini* sous Windows), XML ou encore '*.properties*' (standard java).

14.2.8. Pistes à suivre

Les pistes à suivre pour permettre d'apporter une réponse aux nombreuses questions restées ouvertes ci-dessus ne manquent pas.

Au niveau RTP, puisque RTP n'est en fait une librairie de fonctions, nous devrions investiguer du coté de ses interfaces de programmations: peut-être, après tout, n'est-il pas si compliqué de générer des paquets RTP/RTCP puis de les envoyer vers une servlet.

Pour ce qui est de java, l'étude et l'utilisation de Java Media Framework (JMF) nous paraît incontournable (JMF comprend le package javax.media.rtp). Au moment d'écrire ces lignes, JMF en est à sa version 2.1.1. et la présentation qui en est faite sur http://java.sun.com/products/java-media/jmf/ nous livre le texte suivant:

> *The Java Media Framework API (JMF) enables audio, video and other time-based media to be added to Java applications and applets. This optional package, which can capture, playback, stream and transcode multiple media formats, extends the multimedia capabilities on the J2SE platform, and gives multimedia developers a powerful toolkit to develop scalable, cross-platform technology.*
>
> *JMF 2.1.1, the latest release, simplifies RTP usage, ...*

Pour ce qui est de SSL, les sources d'informations ne manquent pas et nous avons même découvert des logiciels permettant l'encapsulation de flux très divers en SLL; une de nos principales sources d'informations - voire d'inspiration - en la matière sera bien entendu http://www.stunnel.org (Stunnel - Universal SSL Wrapper). Quant à notre idée d'encapsuler du trafic RTP, elle n'est pas vraiment neuve, comme en témoigne le nombre de références trouvées sur l'Internet dont voici quelques extraits:

> *Rtptunnel is a program for tunneling RTP traffic through a TCP connection. You might find it useful if you're behind a firewall that doesn't let UDP packets through. It's really a one-day hack I wrote to talk to someone behind a firewall.*
> http://gphone.sourceforge.net/template.php3?page=rtptunnel
>
> *The solution implemented here* (NOTE: en java, code source inclu) *is to tunnel UDP packets back to RAT through a TCP stream.*
> http://home.comcast.net/~cgokey/java/rtptunnel/
>
> *There is a need for tunneling RTP streams inside RTSP* (NOTE: protocole de contrôle décrit dans [RFC2326]) *in HTTP because in some cases users are located behind a firewall that is configured to only let HTTP through.*
> *http://www.dmn.tzi.org/ietf/mmusic/51/id/draft-gentric-avt-rtsp-http-00.txt (IETF draft, Janvier 2001)*

14.3. Organisation des fonctions périphériques

14.3.1. Développement

Les principales exigences qui concernent le développement traitent du lieu (13.4.11.a), de la méthode (13.4.11.b) (13.4.11.c) et des outils (13.4.11.b).

Pour ce qui est du lieu (13.4.11.a), nous avons établi que le sous-système *local* (13.1.3.a) ne présentait pas des garanties de sécurité optimales (5.2.4.1.h); notre position consisterait donc, après un rapide audit consacré notamment aux procédures de sauvegarde[187] et à l'accessibilité des locaux et machines[188], à considérer que le sous-système *distant* (13.1.3.a) que constitue le domicile de l'employé responsable du développement

[187] Du fait de l'incertitude quant à la sécurité physique des sous-systèmes distants (8.2.2.d), ces sauvegardes devront être effectuées vers le sous-système serveur.

[188] Dans le but d'infirmer nos hypothèses préalables concernant l'accessibilité des sous-systèmes distants (8.2.3.g) (8.2.3.h).

présenterait probablement un meilleur niveau de sécurité. Cette option infirme une des hypothèses que nous avions établies au chapitre 5 (5.2.4.1.e).

La méthode (13.4.11.b) (13.4.11.c) de développement doit nous permettre de travailler par incréments de petite taille - voire par prototypes, lesquels devront être validés et testés indépendamment les uns des autres avant assemblage final et tests d'intégration. Cette manière de procéder, prudente, nous paraît incontournable dans un projet où le risque technologique[189] est majeur, et dans ce contexte un modèle de cycle de vie en spirale paraît approprié.

Au niveau des outils, une solution idéale serait probablement de disposer d'une suite intégrée comme en propose IBM: la suite *Rational*, anciennement *Rational Rose*[190]. Ces outils permettent souvent la prise en charge du processus complet depuis l'analyse des exigences jusqu'à la gestion des versions en passant par la génération partielle de code à partir de diagrammes UML. Toutefois, outre le coût (13.4.15.b) d'une telle solution, son premier effet serait probablement d'alourdir encore davantage la courbe d'apprentissage de la ou des personne(s) impliqué(e)s. Nous préférerons donc, pour ce qui est des outils, en rester sobrement à notre environnement traditionnel: un IDE (en l'occurrence VisualAge for Java, de IBM[191]) et un outil de gestion de configuration (GNU CVS[192]).

14.3.2. Déploiement

Même strictement limité aux protocoles et technologies utilisés, le Java Media Framework (JMF) reste probablement quelque chose d'assez volumineux qui pourrait bien imposer une installation préalable sur les postes clients, contrevenant ainsi partiellement à notre exigence d'automatisation du déploiement des modules client (13.4.12.c).

Enfin, l'exigence de non modification de la configuration des dispositifs de protection logique du siège central de l'entreprise (13.4.12.b) n'est pas rencontrée dans le type d'architecture envisagé ci-dessus, puisqu'il est nécessaire, au niveau des filtres à l'entrée de la DMZ, d'autoriser les connexions entrantes sur le port 443 de notre nouveau serveur. Mais il s'agit là d'une opération assez simple, et qui ne devrait être exécutée qu'une fois à un seul endroit.

14.3.3. Maintenance

Les exigences liées à la maintenance font déjà partie de la culture de l'entreprise. Toutes les anomalies constatées, l'explication de leur(s) cause(s) et leur solution sont systématiquement répertoriées et détaillées à l'aide d'un outil comme bugzilla[193]; toutes les opérations de maintenance matérielle ou logicielle (systèmes d'exploitation et configuration) sont consignées dans un journal, et les versions des produits sont gérées via GNU CVS[194]. Lorsqu'ils existent, les liens entre le numéro du "bug" (dans bugzilla) d'une part et le numéro de ligne (du journal) ou le "tag"/la "révision" (dans GNU CVS) sont systématiquement répertoriés.

[189] Le risque technologique lié à un projet représente la probabilité que le projet échoue du fait de la complexité des technologies mises en oeuvre et/ou du manque de maîtrise des dites technologies par le personnel du projet.
[190] http://www.rational.com
[191] http://www.software.ibm.com/vajava
[192] http://www.cvshome.org/
[193] http://www.mozilla.org/projects/bugzilla/
[194] http://www.cvshome.org/

Chapitre 15 Mode d'acquisition

Nos exigences sont connues, et leur transcription en architecture du produit esquissée. C'est le moment de décider du mode d'acquisition du produit: développement *intra muros* ou package standard ?

15.1. Introduction

Trouver sur le marché un produit qui satisfasse nos besoins est une perspective qui mérite bien que nous fassions quelques concessions quant aux exigences énoncées. D'abord parce que, économiquement, il n'est pas toujours justifié ni réaliste de réinventer la roue si on en trouve de toutes faites à bon prix, mais aussi parce que telles qu'énoncées, nos exigences dessinent une application exactement à nos mesures pour laquelle il est improbable qu'un équivalent puisse être trouvé sur le marché.

Nous allons donc dans un premier temps établir une liste minimaliste de critères de sélection en remontant directement aux motivations premières de nos exigences du chapitre 13[195]. Ensuite, nous procéderons à un rapide échantillonnage (sans prétention de complétude ni de représentativité) via l'Internet de quelques produits que nous évaluerons sur base de notre liste de critères afin de nous positionner par rapport à l'offre rencontrée. Pour terminer, nous prendrons et motiverons la décision relative au mode d'acquisition du produit.

15.2. Critères d'évaluation retenus

15.2.1. Critères relatifs à la confidentialité

Notre objectif minimum de sécurité par rapport à la confidentialité[G] est double:

- *(15.2.1.a)* garantir la confidentialité[G] du contenu des conversations, ce qui équivaut à exiger que les sessions[G] soient chiffrées (4.4.3.h) et que le serveur de l'application, si serveur il y a, soit opéré par l'entreprise en ses locaux (4.4.3.f);
- *(15.2.1.b)* ne pas permettre à un client de découvrir l'identité des autres clients (4.4.3.a), ce qui impose que le répertoire soit personnel, non dynamique (pas de recherche automatique via un protocole de signalisation ou des serveurs LDAP) et configuré pour chacun par un employé de l'entreprise.

Notons au passage que si nous voulons que le répertoire de chaque utilisateur soit géré par un employé de l'entreprise, il nous semble difficile de gérer et maintenir ceux-ci dans une application qui ne disposerait pas d'un serveur où ces répertoires seraient centralisés.

15.2.2. Critères relatifs à l'intégrité

Nos craintes par rapport au critère d'intégrité[G] tournaient toutes autour de l'intégrité[G] du code source et des données persistantes. Par rapport à ces craintes, les mesures minimales qu'il nous semble devoir envisager pour bénéficier de garanties raisonnables consistent à:

- *(15.2.2.a)* exiger que les données persistantes soient placées sous le contrôle et la responsabilité d'un employé de l'entreprise (4.7.3.d), ce qui induit l'existence d'un serveur, et
- *(15.2.2.b)* exiger une nouvelle fois que ce serveur de l'application, si serveur il y a, soit opéré par l'entreprise en ses locaux.

Ce édictant, nous faisons l'impasse sur l'intégrité[G] du code source des modules clients de l'application.

[195] Ce jeu minimum de critères sera réduit au point que la plupart d'entre eux proviendront directement des méthodes les plus simples de détermination des besoins de sécurité et d'identification des menaces que nous avons utilisées au début de ce document.

15.2.3. Critères relatifs à l'écologie

Enfin, pour ce qui est de notre critère d'écologie[G], nous rappellerons la nécessité d'éviter de devoir apporter des modifications à la configuration des dispositifs de protection logique des clients[196] *(15.2.3.a)* et celle de disposer d'un mécanisme (interne à l'application) de contrôle de la bande passante utilisée *(15.2.3.b)*.

15.2.4. Critères relatifs à la disponibilité

Outre les diverses mesures organisationnelles sur lesquelles nous ne reviendrons pas, la disponibilité[G] de l'application dépend de quatre facteurs principaux:

- *(15.2.4.a)* que tous les utilisateurs sous Windows puissent avoir accès à l'application (restriction par rapport à (3.4.14.b));
- *(15.2.4.b)* que l'application ne se sature pas elle-même, et donc qu'elle soit un tant soit peu paramétrable au niveau de sa capacité (4.3.3.g) (4.3.3.h);
- *(15.2.4.c)* que les utilisateurs ne puissent enrichir eux-mêmes leur répertoire ou utiliser l'application pour entrer en contact avec des personnes ne figurant pas dans leur répertoire (utilisation illicite des ressources informatiques: tableau 6.7 (6.4.4));
- *(15.2.4.d)* que personne ne puisse s'inscrire soi-même et devenir utilisateur.

Contrairement à ce que nous avons fait jusqu'à présent, nous ne prenons plus en considération la portabilité pour les clients (15.2.4.a) (dans la mesure où l'immense majorité des postes de travail de l'entreprise et de ses clients tournent sous une version de Windows ou une autre), mais le seul fait de tenir compte des caractéristiques habituelles d'un poste client[197] et de notre première exigence écologique (15.2.3.a) impose que les sessions[G] transitent toutes par un serveur d'application public. Les trois autres facteurs prennent donc tout leur poids dans la mesure où ledit serveur de l'application existe, est effectivement opéré par l'entreprise en ses locaux et qu'une part importante des sessions[G] passe par lui.

15.2.5. Critères relatifs à l'imputabilité

En ce qui concerne l'imputabilité[G], nous nous bornerons à exiger l'identification[G] et l'authentification[G] des utilisateurs par une méthode qui soit au minimum du niveau de CHAP (utilisation, grâce au *challenge*, d'un OTP) *(15.2.5.a)*.

15.2.6. Autres critères

Toutes choses étant égales par ailleurs, préférence sera donnée à la solution la moins coûteuse *(15.2.6.a)*.

15.2.7. Résumé des critères retenus

La liste des critères retenus est reprise au tableau 15.1.

Tableau 15.1	**Liste minimaliste de critères de sélection**	
Identifiant	*Exigences*	*Implémente ou complète*
(15.2.7.a)	Les utilisateurs doivent être enregistrés au niveau de l'application (ceci ne vise pas l'enregistrement commercial auprès du fournisseur).	
(15.2.7.b)	L'enregistrement des utilisateurs est du ressort exclusif d'un employé de l'entreprise	*(15.2.4.d)*
(15.2.7.c)	L'utilisation du SC n'est possible qu'après identification et authentification.	*(15.2.5.a)*
(15.2.7.d)	L'authentification doit au minimum mettre en oeuvre une technique impliquant un OTP.	*(15.2.5.a*

[196] Il serait dénué de sens de vouloir nous montrer plus exigeants ici que nous ne l'étions lors de l'esquisse de l'architecture (14.3.2).

[197] Rappelons qu'un poste client typique ne dispose pas nécessairement d'une adresse IP fixe et qu'il n'est pas prévu, au niveau des dispositifs variés de protection logique, qu'il puisse être joint par des connexions entrantes (*incoming requests*).

Tableau 15.1	**Liste minimaliste de critères de sélection**	
Identifiant	*Exigences*	*Implémente ou complète*
(15.2.7.e)	L'application devra fonctionner par l'intermédiaire d'un serveur accessible via l'Internet.	(15.2.4.a)
(15.2.7.f)	Le serveur sera hébergé dans les locaux de l'entreprise et opéré par l'entreprise.	*(15.2.1.a)* *(15.2.2.b)*
(15.2.7.g)	Les données persistantes de l'application seront conservées au niveau du serveur.	*(15.2.2.a)*
(15.2.7.h)	Une limite supérieure d'utilisation de la bande passante doit pouvoir être configurée et respectée par l'application.	*(15.2.3.b)* *(15.2.4.b)*
(15.2.7.i)	Toutes les communications seront chiffrées.	*(15.2.1.a)*
(15.2.7.j)	Le répertoire est individuel, mais chaque répertoire individuel n'est composable et modifiable que par un employé de l'entreprise.	*(15.2.1.b)*
(15.2.7.k)	Aucun utilisateur ne pourra inviter d'autres personnes que celles qui figurent dans le répertoire.	*(15.2.4.c)*
(15.2.7.l)	La partie cliente de l'application doit tourner sous Windows.	*(15.2.4.a)*
(15.2.7.m)	L'application doit être exploitable sans modification de la configuration des dispositifs de protection logique au niveau des clients.	(15.2.3.a)
(15.2.7.n)	Si possible, éviter ou limiter les coûts en matériel(s) et logiciel(s)	(15.2.6.a)

15.3. Présélection des produits

Même en nous limitant d'emblée, comme nous l'avons fait, aux produits dont la partie *client* fonctionne sous Windows (15.2.7.l), le nombre de produits trouvés sur l'Internet en relativement peu de temps est tellement important qu'il est difficile d'en sélectionner un échantillon représentatif. D'après ce que nous avons découvert, ces produits peuvent être répartis grossièrement en trois catégories principales:

- la catégorie des produits qui proposent la communication vocale en mode *peer to pee*' comme fonctionnalité accessoire ou additionnelle par rapport à leur finalité première. Dans cette catégorie, que nous n'avons pas sélectionnée, citons par exemple *NetOp Remote Control*[198];
- la catégorie des produits dont la finalité va de la simple communication (audio, vidéo) à la collaboration (transfert et/ou partage de documents, chat, etc.) via l'Internet: très diversifiée, tant du point de vue des fonctionnalités que des technologies utilisées, c'est dans cette catégorie qu'il nous semble avoir le plus de chances de trouver notre bonheur et, sans surprise, c'est à elle que se rattachent la plupart des produits que nous avons souhaité confronter à nos critères: *NetMeeting*, *FreePhone*, *Groove Workspace*, *RAT* et *VoiceWeaver*;
- enfin, la catégorie des produits qui s'affichent ouvertement comme ciblant la téléphonie via IP: la plupart des produits de cette catégorie tendent à nous proposer des services comparables à ceux que nous offre un combiné téléphonique évolué, et permettent également par l'intermédiaire d'un ITSP de joindre un correspondant sur son téléphone classique: nous avons choisi d'illustrer cette catégorie avec *Internet Phone*.

Typiquement, les produits de cette dernière catégorie sont des produits commerciaux qui s'appuient sur toutes les possibilités de la signalisation pour choisir et emprunter la passerelle adéquate entre le monde de l'Internet et celui de la téléphonie classique (*PC to Phone*), mais ils mettent aussi souvent à disposition de leurs utilisateurs un serveur public à vocation de répertoire Internet pour le mode *PC to PC*. Ce sont aussi ces produits qui, paradoxalement peut-être et pour ce dernier mode, semblent offrir le moins de compatibilité entre eux.

[198] http://www.netop.com

15.4. Evaluation des produits

15.4.1. NetMeeting (NM)

NetMeeting (de MicroSoft[199]) est disponible gratuitement sur pratiquement toutes les plates-formes Windows. Cet outil permet à n'importe quel utilisateur de converser (entre autres fonctionnalités) avec n'importe quel correspondant via l'Internet, et ce directement (en mode *peer to peer*). La recherche d'un correspondant peut, notamment, s'effectuer grâce à un serveur d'annuaire (LDAP) où chacun est libre de s'inscrire.

NetMeeting utilise également toute une série de ports TCP[200], en plus des ports UDP assignés directement pour RTP (1024-65535), ce qui en fait un outil très délicat à utiliser derrière des dispositifs de protection logique. Lorsque il nous arrive d'utiliser cet outil, une machine *conférence* est placée à cette fin directement dans notre DMZ.

Enfin, les sessions[G] *NetMeeting* ne sont pas chiffrées par défaut, et si le chiffrement est possible (établissement de connexions dites sécurisées), cela ne concerne que les données et pas la voix[201].

15.4.2. Groove Workspace (GWS)

Groove Workspace (de Groove Networks[202]) est la partie *client* d'un puissant logiciel de collaboration offrant également la possibilité de converser en ligne (mais toutefois pas en duplex intégral). Le concept ici est un peu différent, basé sur la notion *d'espace de travail* créé par un utilisateur et auquel on ne peut obtenir le droit d'accès (permanent) que sur invitation[G]. Ce mode de fonctionnement pourrait couvrir un de nos soucis par rapport à la confidentialité[G] (15.2.1.b) si nous créions, par exemple, un espace de travail par client. Malheureusement, il faudrait alors un employé à l'écoute dans chaque espace de travail.

Groove Workspace fonctionne sur le principe du mode *peer to peer* lorsque cela est possible (dans un LAN, par exemple); dans le cas contraire les échanges s'effectuent via un *relay*, serveur sur Internet auquel les clients s'adressent directement, ce qui permet à la fois de traverser les dispositifs de protection logique avec ou sans *proxy* http (*Groove Workspace* réalise une encapsulation HTTP) mais aussi de conserver (sous forme différentielle) les modifications apportées par un utilisateur pour permettre la synchronisation différée entre tous les *clients* du même workspace lorsqu'ils ne sont pas *on line* simultanément.

Le serveur (*Groove Enterprise Relay*) offre quelques fonctions de reporting de l'activité, mais rien nous semble-t-il qui puisse nous permettre de limiter l'utilisation globale de bande passante.

Du point de vue de la confidentialité[G], toutes les communications sont chiffrées; par contre, au niveau de l'imputabilité[G], aucune garantie réelle n'existe par défaut puisque chaque utilisateur s'enregistre lui-même localement sous le nom qu'il souhaite.

Groove Workspace revient à 69 USD (par copie), prix auquel il faut ajouter le prix du serveur (*Groove Enterprise Relay*).

15.4.3. FreePhone (FP)

FreePhone[203] est une initiative du groupe de recherche IP Audio de l'INRIA[204]. Disponible gratuitement, il fonctionne sous Windows comme sous plusieurs plates-formes Unix. Cet outil permet à n'importe quel

[199] http://www.microsoft.com
[200] 389/TCP (Internet Locator Server), 522/TCP (User Location Server), 1503/TCP (T.120), 1720/TCP (H.323 call setup) et 1731/TCP (Audio call control)
[201] En pratique, la fonctionnalité de communication vocale semble même tout simplement inhibée en cas de chiffrement de la session.
[202] http://www.groove.net
[203] http://www.inria.fr/rodeo/fphone
[204] Institut National de Recherche en Informatique et en Automatique, France, http://www.inria.fr

utilisateur de converser (entre autres fonctionnalités) avec n'importe quel correspondant via l'Internet, et ce directement (en mode *peer to peer*). *FreePhone* ne fournit pas de fonctionnalité de recherche d'un correspondant, mais chaque utilisateur peut composer son répertoire à sa guise.

FreePhone ressemble assez à *NetMeeting*, à ceci près qu'il ne fonctionne pas en duplex intégral et que son code source peut être obtenu sur demande. Nous n'avons pas non plus trouvé beaucoup d'informations techniques détaillées, mais l'outil ne semble pas prévoir de possibilité d'encapsulation: un rapide essai dans notre LAN domestique nous a permis de constater, outre la paire de ports UDP assignée dynamiquement pour RTP, que du trafic avait également été échangé via un autre port (5003/udp), ce qui peut rendre problématique son utilisation derrière nos dispositifs de protection logique.

Enfin, le site Internet consulté ne nous fournit aucune information quant à l'éventuel chiffrement des sessions[G].

15.4.4. Internet Phone (IPH)

Considéré naguère par certains comme le leader ou la référence du marché, *Internet Phone* de VocalTec[205] est un outil très complet de téléphonie permettant de contacter aussi bien un téléphone normal (via un ITSP) qu'un autre PC depuis l'Internet. Un serveur de VocalTec fournit le service de répertoire (ouvert à tous) via un *community browser*, mais ce service n'est pas nécessaire et il est possible d'appeler quelqu'un directement par exemple via son adresse IP. L'utilisation de *Internet Phone* derrière nos dispositifs de protection logique peut requérir l'ouverture de plusieurs ports[206] selon l'usage qui en est fait, et nous ne sommes pas parvenus à déterminer si les communications étaient chiffrées ou non.

Internet Phone reviendrait à plus ou moins 50 USD par client, mais ces informations remontent à 1999 et aujourd'hui, le site de VocalTec semble ne plus faire état du produit.

15.4.5. Robust Audio Tool (RAT)

Robust Audio Tool[207] est un impressionnant outil de conférence audio *open source* qui peut être exécuté sur plusieurs versions de Windows et de Unix/Linux. Contrairement à la plupart des autres produits, *RAT* ne s'occupe que de la gestion des flux audio (RTP/RTCP) et ne contient aucune fonction de répertoire ni de signalisation (recherche et invitation[G] des correspondants,..). Il est donc conçu pour être utilisé avec (et lancé par) un logiciel séparé[208] qui prendrait ces fonctions en charge et lui fournirait au minimum l'adresse IP du correspondant ainsi que le premier numéro de port UDP (pair) à utiliser.

Mais les points forts de *RAT* ne se limitent pas à cette séparation des fonctions: depuis la ligne de commande, *RAT* peut être démarré avec un vaste choix d'options, comme par exemple la clé de chiffrement à utiliser (DES) ou encore le mode de fonctionnement: *RAT* peut, si on lui fournit deux paramètres au format *adresse*[209]*/port/ttl/codec*, assumer le rôle de *translator* ou de *mixer*. Le lecteur intéressé trouvera la documentation (*man pages*) de *RAT* en ANNEXE 18.

RAT est un produit du *Department Of Computer Science*, de l'*University College of London*.

15.4.6. VoiceWeaver (VW)

VoiceWeaver[210] est une boîte à outils qui vous aide à créer un script PHP que vous pouvez ensuite déployer sur tout serveur web digne de ce nom. L'utilisateur qui le souhaite et y a été enregistré se connecte à votre site, s'identifie et s'authentifie, puis accède à un répertoire dans lequel, parmi sa liste de contacts, ceux qui sont connectés sont clairement distinguables des autres; il lui suffit ensuite d'y choisir un correspondant parmi ceux qui sont disponibles, de l'inviter et, si réponse il y a, une conversation (chiffrée) s'engage.

---

[205] http://www.vocaltc.com

[206] 6670/tcp (internet phone servers), 22555/udp (communications), 25793/tcp (addressing server), 1490/tcp (conference engine).

[207] http://www-mice.cs.ucl.ac.uk/multimedia/software/rat

[208] Par exemple via *Session Directory Tool* (SDR): http://www-mice.cs.ucl.ac.uk/multimedia/software/sdr

[209] Unicast ou multicast

[210] http://www.voiceweaver.com

Vu de plus près le tableau est un peu moins idyllique: la contribution du site web se limite à délivrer un *plug-in* qui ne fonctionne que sous IE et permet d'établir une communication en pur *peer to peer* direct de *client* à *client*: les ports 1300/tcp, 5000/udp et 5001/udp de chaque *client* doivent être ouverts, et même largement ouverts (*outgoing to any ip destination, incoming from any IP spource*). Sans parler du problème des sous-systèmes *distants* (13.1.3.a) qui hébergent un réseau local[211] comportant deux ou plus de deux clients: ces machines *clientes* ne sont pas directement connectées à l'Internet (elles ne disposent d'habitude que d'une adresse IP privée qui est convertie en sortie[212]), ce qui ne permet même pas de les rendre accessibles par la configuration en entrée de règles de *destination natting* (DNAT) puisqu'il n'existe, a priori, aucun moyen de savoir vers quel client rediriger le trafic entrant *(15.4.6.a)*.

VoiceWeaver ne supporte pas non plus la notion de groupe d'utilisateurs, ce qui signifie que si le répertoire peut effectivement être imposé par un administrateur, il sera néanmoins le même pour tous les utilisateurs. Une manière de contourner cet obstacle consisterait à construire autant d'instances (serveurs web virtuels) du site *VoiceWeaver* que nous souhaitons avoir de groupes d'utilisateurs différents, ce qui équivaudra à créer autant d'instances que nous aurons de clients distincts, à inscrire chaque employé dans chaque instance, à convaincre chaque employé qui souhaite se connecter à le faire dans toutes les instances et, *last but not least*, à devoir probablement s'acquitter du *fee* (99 USD) une fois par instance.

A part cela, *VoiceWeaver* est ce qui se rapproche le plus de nos attentes, et l'éditeur du produit semble envisager prochainement une version *business* pour répondre au besoin des groupes d'utilisateurs: si cette version permet à un utilisateur de participer à plusieurs groupes, et donc de ne se connecter qu'une fois, ce sera un bon pas dans la bonne direction.

15.4.7. Autres produits

Dans la deuxième de nos catégories (15.3), d'autres produits peut-être moins connus mais tout aussi intéressants méritent d'être mentionnés. Nous pensons par exemple au très complet et séduisant *SpeakFreely*[213] qui fonctionne sous Windows comme sous Unix et est *open source* (mais pas *firewall friendly*[214])

Dans la catégorie des produits de téléphonie via IP, illustrée par *Internet Phone*, nous ne résistons pas à signaler l'originalité d'un produit comme *MediaRing Talk*[215]: outre les appels vers un téléphone normal, *MediaRing Talk* permet d'établir une session[G] de *PC à PC* sans que le destinataire soit connecté à l'Internet. L'appelant se sert de son modem et du numéro de téléphone du modem du PC destinataire pour réveiller l'instance de *MediaRing Talk* qui y tourne (2 ou 3 sonneries); les deux machines se connectent alors à un serveur sur l'Internet (éventuellement via un *proxy* http, d'où encapsulation) et la conversation commence. Dans cette même catégorie citons encore *WebCall* [216] qui vous appelle vous et votre correspondant au tarif local depuis l'Internet, *PC-Telephone*[217], *Net2Phone*[218], et bien d'autres encore ...

Une autre catégorie de produits que nous avions exclus d'emblée de notre évaluation sont les produits dont la partie *client* (ou *peer*) ne fonctionne pas sous Windows (15.2.7.1). Cette catégorie ne manque pourtant pas d'intérêt, ne serait-ce que pour le caractère *open source* d'une partie de ses représentants, qui leur confère une prodigieuse valeur d'exemplarité. Parmi la liste de ces produits, nous épinglerons tout spécialement *Gnome Meeting*[219]: écrit par un étudiant de l'UCL[220] dans le cadre d'un travail de fin d'études, *Gnome Meeting* est un client H.323 pour Linux (environnement graphique) distribué sous licence GNU/GPL. Mais nous nous en

---

[211] Sans chercher très loin, c'est le cas chez nos plus gros clients (nos clients ASP) ainsi qu'à notre propre domicile.

[212] Les adresses privées sont toutes habituellement converties en une seule adresse publique (NAT: *Network Address Translation*, souvent nommé *maquerading* lorsque l'adresse publique est dynamique).

[213] http://www.speekfreely.org

[214] Un logiciel ou une application est souvent qualifiée de *firewall friendly* lorsque son exploitation n'impose pas de modification de configuration au niveau des dispositifs de protection logique.

[215] http://www.mediaring.com

[216] http://www.betsnetcall.com

[217] http://www.pc-telephone.com

[218] http://www.net2phone.com

[219] http://www.gnomemeeting.org

[220] Université Catholique de Louvain: http://www.ucl.ac.be

voudrions aussi de passer ici sous silence des projets comme *Gphone*[221], *Linphone*[222], *Vat*[223] ou encore *NetVot*[224].

15.5. Synthèse

Le tableau ci-dessous reprend en résumé les critères que nous avons établis et, pour chacun des 6 produits présentés, renseigne le respect ou non de ces critères.

Tableau 15.2	**Liste minimaliste de critères de sélection**					
Exigences	*NM*	*GWS*	*FP*	*RAT*	*IPH*	*VW*
Enregistrement des utilisateurs (15.2.7.a)	non	non	non	non	non	oui
Impossibilité de l'auto-enregistrement (15.2.7.b)	non	non	non	non	non	oui
Identification et authentification (15.2.7.c)	non	locales	non	non	non	oui
Authentification au minimum via un OTP (15.2.7.d)	non	-	non	non	non	?
Utilisation d'un serveur (15.2.7.e)	non	oui	non	possible	non	pour login et répertoire
Serveur hébergeable (15.2.7.f)	non	oui	non	possible	non	pour login et répertoire
Données persistantes sur le serveur (15.2.7.g)	non	non	non	non	non	oui
Configuration globale de la bande passante autorisée (15.2.7.h)	non	non	non	non	non	peut-être[225]
Chiffrement des communications (15.2.7.i)	non	oui	?	oui	?	oui
Répertoire individuel au contenu imposé (15.2.7.j)	non	non	non	-	non	pas individuel
Possibilités de communication limitées aux correspondants du répertoire (15.2.7.k)	non	non	non	-	non	oui
Le client ou *peer* tourne sous Windows (15.2.7.l)	oui	oui	oui	oui	oui	oui
Firewall friendly (15.2.7.m)	non	oui	non	non	non	non
Prix (15.2.7.n)	gratuit	69 USD par client	gratuit	gratuit	50 USD par client	99 USD (par groupe ?)
Particularités intéressantes						
Code source disponible			sur demande	*open source*		
Fonctionnement en mode *translator*				oui		
Fonctionnement en mode *mixer*				oui		
Disponible sous Linux			oui	oui		serveur
Signalisation dissociée				oui		

[221] *Gnome-o-Phone*: http://gphone.sourceforge.net. A ne pas confondre avec le *GphoneBuddy Service* (http://www.vliusa.com)

[222] http://www.linphone.org

[223] *Vat* est utilisable sur presque toutes les Unixes: http://www-nrg.ee.lbl.gov/vat/vat.html

[224] *NETwork Voice Terminal*: http://charon.minilab.bdeb.qc.ca/inf850/yickkk/produits.htm

[225] Il devrait être possible, en modifiant le script PHP généré, de limiter le nombre de sessions concurrentes. Notons toutefois que comme les sessions ne passent pas par le serveur, seules celles auxquelles participe au moins un employé travaillant dans le sous-système *local* empruntent la ligne louée de l'entreprise; la pertinence de ce critère s'en trouve donc quelque peu atténuée.

Notre première impression suite à ce rapide survol de quelques références est une certaine surprise d'avoir découvert, même si nous les avons parfois ignorées[226], une telle abondance de solutions disponibles sous Linux/Unix. Passé ce cap, nous constatons que si certains produits implémentent effectivement une technologie d'encapsulation HTTP avec connexion vers un serveur à fonction de *relay*, aucun de ceux que nous avons rencontrés ne permet d'établir et de gérer de manière centralisée des répertoires personnalisés pour les utilisateurs - or ce mode de gestion des répertoires correspond à une de nos exigences les plus importantes. La plupart au contraire, et c'est bien compréhensible, multiplient les possibilités de trouver de nouveaux correspondants, parfois même en collectant et centralisant des informations sur les centres d'intérêts des différents utilisateurs tenus de s'enregistrer.

Tout ceci bien entendu ne fait pas notre affaire, puisque la perspective de parvenir à éviter un développement long et difficile semble devoir s'éloigner. *VoiceWeaver*, le plus proche de nos aspirations, présente peut-être quelques faiblesses (comme cela pourrait être le cas de la méthode d'authentification[G] [227]) mais pose surtout encore deux problèmes majeurs qui sont l'unicité du répertoire et l'obligation de reconfigurer les dispositifs de protection logique du sous-système *local* (13.3.1.a) et de tous les sous-systèmes *distants* (13.1.3.a) en se limitant à un client par sous-système (13.1.3.a) pour cause de limitation inhérente au DNAT comme expliqué plus haut (15.4.6.a).

15.6. Mode d'acquisition

La disponibilité en *open source* d'excellents produits comme *RAT*, caractérisé entre beaucoup d'autres choses par sa modularité, sa versatilité et le nombre de CODECs supportés, constitue une excellente surprise et devrait nous permettre de dégager une voie médiane entre les deux extrêmes que sont le développement sur mesure (difficile, voire dangereux (7.3.4.a)) et le produit du marché (insatisfaisant).

En effet, si nous regardons les choses à une certaine distance, il ne manquerait à *RAT* pour nous satisfaire qu'à lui adjoindre notre habillage minimum de gestion de répertoire, de signalisation et d'encapsulation SSL/TLS: nous aurions alors le produit recherché, sauf pour ce qui concerne notre exigence d'automatisation du déploiement sur les postes clients, mais celle-ci n'est probablement pas la plus critique.

De plus, la possibilité de démarrer *RAT* en lui spécifiant les ports UDP à utiliser[228] peut également nous être utile en cas de problèmes de performances liés à l'encapsulation SSL/TLS[229], puisqu'une voie alternative consisterait à revenir vers une session[G] purement UDP, moyennant il est vrai certaines concessions au niveau des dispositifs de protection logique dont nous allons débattre à l'instant.

Au niveau de nos dispositifs de protection logique, ce qui nous ennuie le plus est probablement le fait que les ports UDP utilisés par RTP/RTCP sont assignés dynamiquement. En mode *peer to peer*, cette caractéristique nous obligerait à ouvrir pratiquement tous les ports UDP[230] en (*incoming from any IP/port, to any port*) et (*outgoing to any IP/port from any port*). Le choix de l'architecture client serveur, avec passage obligé et systématique par le serveur, referme légèrement cette fenêtre d'exposition, mais nous restons encore tributaires de la limite de un client du SC par sous-système *local* et distants (15.4.6.a). Par contre, si au niveau des données persistantes conservées dans la base de données du serveur du SC, nous assignons une paire de ports UDP (voire un *range* restreint de ports UDP) par utilisateur, cette information pourrait être communiquée au client du SC une fois l'utilisateur identifié et authentifié, et utilisée pour établir la session[G] RTP/RTCP entre ce client du SC et le serveur du SC avec comme avantage de ne devoir ouvrir, au niveau

[226] Nous n'avons considéré que les solutions qui fonctionnaient sous Windows.

[227] Nous ignorons tout de cette méthode, et comme nous ne sommes jamais parvenus à nous connecter sur leur site de démonstration nous n'avons pas davantage pu regarder ce qui passe sur le réseau au moment de l'authentification.

[228] Il est probable que tous les produits *open source* pourraient être adaptés pour atteindre cet objectif; *RAT* nous dispense simplement de devoir modifier le code (probablement au niveau de la signalisation comme au niveau des API de RTP/RTCP) pour atteindre cet objectif.

[229] Problèmes qui pourraient être la résultante des délais d'encapsulation, de l'overhead (en-têtes TCP) et des caractéristiques de TCP: orienté *connexion fiable*, TCP procède le cas échéant à la réémission des paquets perdus (et *slow start*) avec comme conséquence que le destinataire attend pour pouvoir restituer tous les paquets dans la bonne séquence à l'application, d'où risque de variabilité importante des délais.

[230] Un produit *open source* devrait nous permettre de limiter l'ouverture à un *range* plus restreint.

des dispositifs de protection logique, qu'un nombre limité de ports UDP par site et pour une seule IP externe[231]. De plus, du fait de la prédictabilité des ports utilisés, la configuration de règles de DNAT devient possible et la limite de un client par sous-système *local* et *distants* est levée[232].

Le prix à payer pour une telle configuration n'est toutefois pas à négliger, et sans effectuer de recherche intensive nous identifions déjà 3 inconvénients majeurs:

- nous devrions (faire) adapter la configuration des dispositifs de configuration logique de tous les sous-système local et distants, ce qui signifie:
  - beaucoup de travail;
  - que certains de nos clients seront exclus du SC[233];
  - nous nous exposons au risque[G] d'erreur (7.3.4.a);
- si un utilisateur peut se connecter au SC depuis plusieurs endroits différents, il faudra répéter à chaque place la même configuration des dispositifs de protection logique;
- si un sous-système distant utilise en interne le protocole DHCP sans qu'il existe un lien fixe entre l'adresse IP assignée à un poste client et son adresse MAC, il faudra que le DHCP puisse mettre automatiquement à jour un service de noms, et que le DNAT puisse être configuré dynamiquement sur base du nom des machines et pas de l'adresse IP interne[234].

Le lecteur comprendra donc notre réticence à nous engager dans cette dernière voie si cela ne s'avère pas nécessaire. En conclusions, nous privilégierons donc l'idée précédente qui consistait à utiliser un produit du marché comme *RAT* et à lui ajouter l'habillage nécessaire (développement de la gestion de répertoire, de la signalisation et de l'encapsulation SSL/TLS) pour qu'il satisfasse nos principales exigences, sous réserve d'une évaluation plus sérieuse de la faisabilité technique.

[231] Outgoing: from (local:udp/xxxx) to (IP serveur SC:udp/xxxx)
Incoming: from (IP serveur SC:udp/xxxx) to (local:udp/xxxx)

[232] Incoming: from (IP serveur SC:udp/xxxx) to (local:udp/xxxx) DNAT to (IP client *X* du SC:udp/xxxx)
Incoming: from (IP serveur SC:udp/yyyy) to (local:udp/yyyy) DNAT to (IP client *Y* du SC:udp/yyyy)

[233] Un de nos clients, installé en Belgique, fait partie d'un grand groupe français et leur connexion à l'Internet se fait à Paris où les personnes responsables interdisent tout accès qui n'est pas absolument nécessaire.

[234] Par exemple, le DHCP peut informer dynamiquement un serveur DNS interne du fait que le client *nomClient* (qui sera souvent un nom netbios) s'est vu attribué l'adresse IP *adresseClient*, et que le DNAT puisse être configuré sur base de *nomClient* au lieu de *adresseClient* - ce qui impose en plus que la machine responsable du DNAT ait accès au service DNS interne et que la configuration du DNAT soit dynamique ou postérieure à l'attribution de l'adresse IP. Ces 2 dernières conditions ne sont par exemple pas remplies dans notre propre sous-système *local*.

Conclusions générales

La décision de l'entreprise

Arrivés au terme de cette étude, nous sommes en mesure de fournir des informations relatives au profil et à l'architecture - sous réserve de validation - du système qui correspondrait aux besoins et au projet de l'entreprise tels qu'ils ont été exprimés en première partie de ce document. Toutefois, l'ampleur de la courbe d'apprentissage technologique requise et l'idée que nous pouvons avoir de la durée du développement - ne serait-ce que par rapport au temps déjà consacré à la réalisation de cette étude - semble devoir rendre caduque l'option initiale qui consistait à *développer quelque chose en profitant du temps disponible quand il y en a*: le projet s'étendrait sur de très nombreux mois si pas davantage et le travail, délicat, ne pourrait pourtant se faire que de manière trop décousue. Pour être entamé et efficacement mené à terme, ce projet devra devenir un projet d'entreprise, laquelle devra y assigner des ressources.

Or, qui dit ressources dit investissement, et qui dit investissement dit retour sur investissement. Nos possibilités de retour sur investissement sont a priori de deux ordres: celui des économies que le système, opérationnel, permettra de réaliser mais aussi celui qui est lié aux possibilités de commercialisation du produit fini. Malheureusement, la proposition qui consistait à développer le système sur base d'un produit open source ne permet plus d'espérer, quand bien même il y aurait un marché demandeur pour ce type d'application, beaucoup de retour sur investissement par le biais de la vente de licences puisque l'incorporation de code open source dans un développement implique que le produit développé soit lui-même open source - sauf à bien pouvoir séparer les deux.

Resterait donc à estimer le temps requis pour un éventuel développement, son coût, et à placer dans l'autre plateau de la balance le montant des économies que l'application devrait permettre de réaliser tenant compte du risque que le développement n'aboutisse pas ou que le produit, développé, ne donne pas satisfaction pour des raisons de performances ou autres.

Vu sous cet angle, si nous étions amenés à prendre la décision finale, nous déciderions d'arrêter là l'expérience.

Méthodes et méthode

Incontestablement, dans notre démarche, chacune des méthodes utilisées nous apporté quelque chose mais chacune nous a aussi quelque peu déçu. Nous ne reviendrons pas ici sur l'ensemble des observations et conclusions déjà présentées à la fin des chapitres concernés, mais simplement sur 5 éléments qui nous paraissent constituer l'enseignement principal de ce travail.

Premier de ces éléments, ce concept d'*écologie*[G] *de l'application* comme critère d'évaluation de la sécurité des SI nous paraît relativement novateur et mériter qu'on s'y intéresse. Issu initialement de notre démarche fondamentale au chapitre 4, il s'est à nouveau imposé par le biais d'une de nos critiques les plus importantes quant au fond sur la méthode EBIOS qui, en ignorant le concept de *sensibilité des entités*, n'aurait pas permis d'exprimer un certain nombres d'exigences fondamentales sur la nouvelle application, exigences destinées à empêcher qu'elle n'abuse d'une ressource de son environnement considérée comme critique pour une autre activité totalement indépendante.

Deuxième enseignement de notre étude, la difficulté qu'il y a de mener conjointement une analyse fonctionnelle et une analyse de risques[G] pour une nouvelle application (5.4.1.a). Les deux analyses sont effectuées parfois avec des outils différents et souvent par des personnes ou des équipes différentes sans beaucoup de communication entre elles mais produisent toutes deux un certain nombre d'exigences sur le SC; en bout de course, nous nous trouvons avec deux sources distinctes d'exigences, avec tout ce que cela peut impliquer de contradictions et de problèmes de traçabilité. Comme la plupart des ténors du secteur (les grandes méthodes internationales comme l'ITSEC) sont expressément conçues - et c'est compréhensible -

pour être indépendantes du cycle de vie du produit, aucun rapprochement n'est à attendre de ce côté. Il nous semble donc qu'il incomberait aux éditeurs d'outils CASE ou autre de prévoir eux-mêmes l'implémentation dans leur produit d'au moins une - mais si possible de plusieurs - techniques et méthodes d'analyse des risques[G].

Le troisième enseignement que nous souhaitons tirer est celui de la probable existence, au niveau de ces méthodes, d'une rupture entre ce qui est disponible et utilisable pour de toutes petites structures (nous avons parfois découvert des méthodes d'analyse des risques[G] qui tenaient sur deux feuilles excel) et ce qui est prévu pou les toutes grosses entreprises. Entre les deux, nous avons l'impression qu'un grand vide existe, vide que pourraient combler des initiatives comme celle du CEA, malheureusement pas aboutie.

L'enseignement suivant que nous tirons de cette expérience est le constat de relative vanité - du fait de l'incertitude quant aux résultats - d'une démarche d'analyse des risques menée en solitaire (5.4.1.c), et à plus forte raison si la méthode utilisée s'avère plus confidentielle que prévu (8.4.e) et n'est pas préalablement maîtrisée par l'évaluateur (5.1.5.a).

Concernant notre approche, nous dirions que notre choix initial qui consistait à élargir notre horizon en utilisant - même très sommairement - plusieurs méthodes différentes s'est avéré un choix payant puisque, effectivement, chacune a en partie conforté les résultats des autres en apportant un éclairage et des éléments différents. Bien entendu, nous ne prétendons pas avoir exploré le nombre idéal de démarches qu'il conviendrait de mettre en oeuvre, ni même d'avoir choisi les meilleures ou les plus représentatives. Bien d'autres possibilités existent, parmi lesquelles plusieurs sont ou ont été éditées par le CLUSIF (MARION, MEHARI, MELISA) mais ne sont pas en accès libre (sinon pour les étudiants qui n'exercent pas d'activité professionnelle), ou encore la méthode des COMMON CRITERIA [CC-1] que nous avons étudiée mais pas exploitée parce que disproportionnée par rapport à nos besoins, et bien d'autres méthodes encore dont beaucoup, commerciales, ne sont pas librement accessibles. Mais la plupart, et en tous cas toutes celles citées ici, sont d'une mise en oeuvre trop lourde ou complexe pour être utilisables par des petites PME. Une exception peut-être, non envisagée faute de temps et de place dans cette étude, pourrait bien être la méthode OCTAVE (http://www.cert.org) dont une version semble destinée aux petites et moyennes organisations.

Pour terminer, nous dirions que notre choix initial qui consistait à garantir la traçabilité de nos exigences par l'insertion et le rappel systématique de marqueurs, s'il ne perturbe plus trop la lecture une fois l'habitude prise, s'est avéré extrêmement difficile à assumer. Non, à notre sens, que le principe soit à reconsidérer - puisqu'il nous semble évident qu'en phase de maintenance par exemple, une telle traçabilité est seule de nature à garantir la pérennité du niveau de sécurité de l'application - mais du fait que nous ne disposions d'aucun outil permettant de supporter efficacement cette fonction. Par exemple, la suite *Rational* (14.3.1) contient des modules qui s'interfacent avec Microsoft Word et permettent de créer efficacement ce genre de lien (sur base d'une simple sélection effectuée dans le texte) mais surtout de les gérer par la suite: déplacement, établissement de matrices de références croisées, etc. Sans l'aide de ce genre d'outil, le travail que cela demande est disproportionné par rapport à la fiabilité qu'il nous semble que nous pouvons attendre du résultat final; le lecteur aura remarqué par ailleurs que nous n'avons pas été en mesure de terminer ce travail avec, de ce point de vue particulier, la même rigueur que celle avec laquelle nous l'avions entamé Clairement, sans outil approprié, nous ne recommencerions pas.

Perspectives

La fin d'un travail n'est souvent rien d'autre qu'une porte ouverte vers d'autres possibilités ou investigations, et le nôtre n'a pas la prétention d'échapper à cette règle. La plus évidente des continuations possibles est probablement celle qui consisterait à envisager malgré tout la conception et le développement de l'application esquissée ici, probablement dans un autre contexte que celui d'une entreprise commerciale, afin de valider - ou d'invalider - la démarche entamée en la poussant à son terme.

Mais à notre avis, le plus intéressant est peut-être ailleurs. Par exemple, ce besoin qu'il nous a semblé pressentir d'un outil ou d'une méthode d'analyse des risques[G] qui soit accessible à des petites et moyennes entreprises nous pousserait à investiguer une des deux voies suivantes:

- entamer méthodiquement une recherche de solution appropriée existante, recherche que nous commencerions par la méthode OCTAVE citée ci-dessus, ou
- envisager d'en élaborer une.

A notre humble avis, une méthode d'analyse des risques[G] abordable pour des petites structures devrait se situer à mi-chemin entre ce qu'a produit le CEA - dont un des points forts reste leurs fiches de recommandations - et une version peut-être plus formalisée mais surtout simplifiée de EBIOS, une version dans laquelle on tenterait de limiter et de simplifier toutes les étapes de quantification qui se sont avéré les plus pénibles et, surtout, les plus sujettes à contestation.

Et puisque nous parlons d'EBIOS pour en dire qu'une version simplifiée serait la bienvenue, profitons également de l'occasion pour signaler que le logiciel d'accompagnement (écrit en java et dont le code source est fourni) n'implémente encore que partiellement la méthode. Il y a assurément, de ce côté, beaucoup de choses utiles et intéressantes à accomplir.

Pour terminer nous ajouterions que la méthode dite des COMMON CRITERIA citée plus haut, en tant que successeur et évolution naturelle de l'ITSEC, mérite certainement le détour. Un des aspects intéressants de cette méthode est la possibilité de définir des *protection profiles*, indépendants de toute implémentation particulière et exprimant les exigences en sécurité pour une catégorie ou un type d'application, ainsi que des *security targets*, lesquels ciblent alors une implémentation bien particulière et peuvent être ou non basés sur un *protection profile* existant. L'exercice consistant à établir un *protection profile* pour un type d'application comme celui que nous avions envisagé, ou le *security target* de cette application serait une démarche intéressante.

Le lecteur intéressé trouvera en ANNEXE 19 l'introduction aux principes des COMMON CRITERIA que nous avions rédigée en investiguant la méthode.

Si c'était à refaire

Au terme de cet itinéraire, si nous devions recommencer nous procéderions en deux étapes.

Dans un premier temps, sur base des travaux du CEA, nous tenterions de mettre au point nous-mêmes une méthode simple et abordable par tous qui puisse être utilisée aussi bien par des patrons de PME disposant d'un vernis informatique que par des professionnels confrontés aux besoins d'établir les besoins de sécurité pour des projets de petite ou de moyenne envergure. La conception (ou finalisation) de cet outil devra impérativement s'accompagner d'une proposition de solution pour une gestion efficace des liens de traçabilité.

Ensuite, dans une seconde phase, nous appliquerions le résultat de ces travaux à notre projet de SC.

Mais si cet itinéraire alternatif nous paraît aujourd'hui plus séduisant, nous avons pleinement conscience que pour avoir pu l'élaborer en deux phrases au paragraphe précédent, le chemin parcouru ici fut probablement nécessaire et, par ailleurs, les paysages rencontrés ne manquaient pas d'intérêt.

FACULTÉS UNIVERSITAIRES NOTRE-DAME DE LA PAIX, NAMUR

INSTITUT D'INFORMATIQUE

RUE GRANDGAGNAGE, 21, B-5000 NAMUR (BELGIUM)

Analyse de risques dans le cadre d'une application distribuée sur l'Internet

Glossaire, Annexes et Bibliographie

Olivier Hislaire

Mémoire présenté en vue de l'obtention du grade de
Licencié en Informatique

Année Académique 2002 - 2003

Table des matières

Second volume

Glossaire

Accès (politique d')
Définition des droits des sujets sur les objets, et de la manière dont ils peuvent être modifiés.

ADSL Asynchronous Digital Subscriber Line.

AES Advanced Encryption Standard.

AH Authentication Header.
Protocole utilisé dans IPSec pour garantir l'intégrité, l'origine et la protection contre le rejeu [RFC2402].

API Application Programming Interface.

Appel
Ensemble des invitations[G] à participer à une même session[G] émanant d'une même source [RFC2543].

ASIRQ Association de la Securité de l'Information de la Region du Quebec (http://www.asirq.qc.ca).

ASP Application Service Provider.

ATM Asynchronous Transfer Mode

Authentification
Processus visant à vérifier si l'identité déclinée par un utilisateur[G] correspond à la réalité.

B2B Business to Business

Besoin de sécurité
Expression a priori des niveaux requis de disponibilité, d'intégrité et de confidentialité associés aux informations, fonctions et sous-fonctions étudiées [EB-G].

Broadcast (diffusion)
Type de communication multidestinataire.

CA Certification Authority.

CASE Computer Aided Software Engineering

CBC Cipher Block Chaining

CC Common Criteria
Critères Communs - officiellement intitulés par l'ISO *Critères d'évaluation de la sécurité des technologies de l'information* [CC-1].

CHAP Challenge Handshake Authentication Protocol
Protocole d'identification et d'authentification décrit dans [RFC1994] et utilisé notamment par PPP.

CLUSIF Club de la sécurité Informatique Français (http://www.clusif.asso.fr)

CODEC CODage - DECodage.
Nom générique de la famille d'algorithmes de codage et de décodage de flux multimédias.

Cohérence
Propriété d'un service ou d'une information, fourni par un SI[G], qui est reproductible (les mêmes causes produisant les mêmes effets) et non contradictoire par rapport à d'autres services ou informations produits par le même système.

Confidentialité (C)
Propriété d'un SI[G] qui assure que seuls les utilisateurs[G] habilités dans les conditions normalement prévues ont accès aux informations.

Conformité
Propriété d'un service ou d'une information, fourni par un SI[G], qui est conforme aux spécifications du SI[G].

Connexion
Ensemble constitué d'un SI, d'un utilisateur identifié et authentifié auprès de ce SI et des flux qui circulent entre eux.

Correction
Propriété d'un service ou d'une information, fourni par un SI[G], dont le résultat ou la valeur est conforme à la réalité.

CSI Computer Security Institute (http://www.gocsi.com)

CTCPEC Canadian Trusted Computer Product Evaluation Criteria

DES Data Encryption Standard

DHCP Dynamic Host Configuration Protocol

DIC (Etiquette ou étiquetage DIC)
Etiquetage des objets informatiques en fonction de leur sensibilité par rapport aux critères d'évaluation de la sécurité que sont la **D**isponibilité[G], l'**I**ntégrité[G] et la **C**onfidentialité[G].

Discrétionnaire (politique d'accès)
Politique d'accès dans laquelle les droits sur les objets peuvent être modifiés à discrétion par les sujets eux-mêmes; ce droit particulier de modification des droits sur un objet est habituellement accordé au propriétaire de l'objet.

Disponibilité (D)
Aptitude d'un SI[G] à pouvoir être employé par les utilisateurs[G] habilités dans les conditions d'accès et d'usage (notamment performancielles) normalement prévues.

DMZ DeMilitarized Zone
Réseau intermédiaire parfois inséré entre un réseau protégé (LAN privé) et un réseau externe en vue de fournir un niveau de sécurité supplémentaire [Chapman].

DNAT Destination Natting.
Modification de l'adresse de destination de datagrammes IP.

DNS Domain Name System.

DoS Deny of Service.
Type d'attaque visant à porter atteinte à la disponibilité[G] d'un SI[G] en saturant ou perturbant une ou plusieurs de ses ressources.

EAL Evaluation Assurance Level.
Ensemble (paquet) de composants d'assurance qui représente un niveau de l'échelle d'assurance prédéfinie des CC [CC-1].

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité.

Ecologie (E)
Propriété qui assure qu'un SI[G] exploité dans les conditions normalement prévues ne puisse porter atteinte à son environnement par l'utilisation non contrôlée d'une ressource[G].

Enrôlement
Processus visant à générer, transférer et enregistrer les informations nécessaires à une identification[G] et/ou authentification[G] ultérieure(s) d'un utilisateur[G] par un autre système.

ERP Entreprise Resource Planning

ESP Encapsulating Security Payload [RFC2406].
Protocole utilisé dans IPSec pour garantir la confidentialité, l'intégrité, l'origine et la protection contre le rejeu.

Exactitude
Propriété qui assure qu'un SI[G] exploité dans les conditions normalement prévues fournit aux utilisateurs[G] habilités des services ou informations qui répondent aux exigences d'utilité[G], de cohérence[G], de conformité[G] et de correction[G].

Fiabilité
Mesure de la continuité de la délivrance d'un service conforme[G].

FTP File Transfer Protocol [RFC959].

GPL GNU Public License.
Contrat de licence de logiciel *open source*.

HDLC High-level Data Link Conrol

HTTP Hyper Text Transmission Protocol [RFC2616].

ICMP Internet Control message Protocol [RFC792].

IDE Integrated Development Environment

Identification
Processus visant à déterminer, parmi plusieurs possibilités, quelle est l'identité d'un utilisateur. L'identification est réussie si l'identité annoncée correspond bien à celle d'un des utilisateurs autorisés.

IETF Internet Engineering Task Force (http://www.ietf.org)

IKE Internet Key Exchange.
Protocole d'authentification, de négociation de clés de chiffrement et d'échange de certificats défini dans [RFC2409].

Imputabilité (W)
Propriété qui permet d'imputer de manière de façon certaine une opération à un utilisateur à un moment donné [CLUSIF1996].

Intégrité (I)
Propriété qui assure qu'une information ou qu'une fonction d'un SI n'est modifiée que par les utilisateurs[G] habilités et dans les conditions d'accès normalement prévues.

Invitation
Action consistant à convier un utilisateur[G] à se joindre à une session[G].

IP Internet Protocol (OSI niveau 3, TCP/IP niveau 2).

IP Hi-jacking
Type d'attaque dans lequel l'attaquant s'insère entre deux entités communicantes, altère les datagrammes au passage et/ou se substitue à une des deux entités une fois celle-ci authentifiée.

IPSec Internet Protocol Security
Protocole de sécurisation des réseaux IP, défini dans [RFC2401].

IT Information Technolgy.
Relevant des technologies de l'information: *un système IT*.

ISDN Integrated Services Digital Line.
En français: Réseau Numérique à Intégration de Services (RNIS).

ISO Organisation internationale de normalization (http://www.iso.org).

ISP Internet Service Provider.

ITSEC Information Technology Security Evaluation Criteria.

ITSP Internet Telephony Service Provider.

ITU International Telecommunication Union http://www.itu.int).

L2TP Layer 2 Tunneling Protocol
Protocole de communication (OSI niveau 2, TCP/IP niveau 1) décrit dans [RFC2661] et conçu pour permettre l'acheminement (par encapsulation) de trames PPP au travers des réseaux interconnectés.

LAN Local Area Network

LDAP Lightweight Directory Access Protocol [RFC3377].

LPD Line Printer Daemon [RFC1179].

MAC Medium Access Channel.

Middle (Man in the middle, substitution)
IP Hi-jacking[G].

Mandataire (politique d'accès)
Politique d'accès dans laquelle les interactions entre sujets et objets obéissent à des règles incontournables qui peuvent être basées, par exemple, sur une classification hiérarchique des objets (sensibilité) et des sujets (niveau d'autorisation).

Menace
Cause potentielle de violation de la sécurité.

Mot de passe
Chaîne de caractères transmise en vue de l'authentification d'un candidat (émetteur de la chaîne) à un serveur d'authentification. Le mot de passe transmis constituer le secret, ou peut être obtenu à partir d'un secret.

MGCP Media Gateway Control protocol [RFC3435].

MIB **Management Information Base**
Base de données reprenant et structurant les objets utilisés par un protocole comme par exemple SNMP. La MIB de SNMP est définie par [RFC3418].

MIME Multipurpose Internet Mail Extensions
Mécanisme pour spécifier et décrire le format du contenu des messages Internet, décrit dans [RFC2045] et [RFC2046].

Multicast **(IP multicast)**
Type de communication pluridestinataire.

NNTP Network News Transfer Protocol [RFC0977].

NSA National Security Agency
Agence fédérale des Etats-Unis (http://www.nsa.gov).

NTP Network Time Prococol [RFC0958].

Objectif de sécurité
Contribution à la sécurité qu'une TOE est destinée à apporter [ITSEC].

Objet (d'un SI)
Entité passive d'un SI, manipulée (création, modification, consultation, suppression) par un ou plusieurs sujet(s)[G]. Selon cette définition, un objet[G] peut également agir en tant que sujet[G].

OTP One Time Pasword.
Se dit d'un mot de passe non réutilisable.

PABX **Private Automatic Branch Exchange.**

PCM Pulse Code Modulation

PHP (Php Hypertex Preprocessor)
Langage open source de script utilisé pour la création de pages web dynamiques.

PP Protection Profile
Ensemble d'exigences de sécurité valables pour une catégorie de TOE, indépendant de son implémentation, qui satisfait des besoins spécifiques d'utilisateurs [CC-1].

PPP Point to Point Protocol
Protocole de communication (OSI niveau 2, TCP/IP niveau 1) pour liaisons point à point initialement décrit dans [RFC1661]], complété par [RFC1162] et [RFC1163].

PPTP Point to Point Tunneling Protocol.

PSTN Public Switched Telephone Network.

RAS Registration, Admission et Status
Protocole de la norme H.225, elle-même chapeautée par le norme H.323 de l'ITU.

RDP Remote Desktop Protocol

Ressource
Ensemble de moyens composant l'architecture technique d'un SI[G] [EB-G]

RFC Request For Comments
Document de l'IETF servant de base à l'établissement des normes et disponibles sur l'Internet..

Risque
Danger ou inconvénient plus ou moins probable auquel on est exposé; le risque est fonction de la menace et des vulnérabilités.

RSA Rivest, Shamir et Alderman.

RSVP ReSerVation Protocol [RFC2205].

RTCP Real-Time Transport Control Protocol
Protocole de contrôle pour RTP.

RTP Real-Time Transport protocol
Protocole de communication s'appuyant sur UDP (OSI niveau 4, TCP/IP niveau 3) initialement décrit dans [RFC1889].

RTT Round Trip time

S/MIME Secure Multipurpose Internet Mail Extensions.
S/MIME est un standard Internet permettant l'échange sécurisé de données de type MIME [RFC1521][RFC1522] et initialement décrit par [RFC1847].

SAP Session Announcement Protocol [RFC2974].

SCSSI Service Central de la Sécurité des Systèmes d'Information.
Ancien service du Premier Ministre de la République Française, créé en 1986 (http://www.ssi.gouv.fr).

SDP Session Description Protocol [RFC2327].

Secret
Chaîne de caractères tenue secrète et destinée à l'authentification d'un candidat (propriétaire et détenteur de la chaîne) à un serveur d'authentification, lequel peut la connaître (secret partagé) ou non (secret non partagé). Le secret peut être transmis comme mot de passe, ou servir à la génération d'un mot de passe non réutilisable (OTP).

Sécurité (politique de)
Ensemble des lois, règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique [ITSEC]. Une politique de sécurité comporte habituellement trois volets: la sécurité physique, la sécurité administrative (définition des rôles) et la sécurité logique.

Session (multimedia)
Ensemble d'émetteurs, de receveurs et des flux multimédias qui circulent de ces émetteurs vers ces receveurs [RFC2327].

SF Security Function
Partie(s) de la TOE sur laquelle (lesquelles) on s'appuie pour appliquer un sous-ensemble étroitement impliqué de règles tirées de la TSP [CC-1].

SFP Security Function Policy
La politique de sécurité appliquée par une SF [CC-1].

SI Système d'Information
Ensemble constitué d'une organisation, de logiciels et de matériels, destiné à accomplir des fonctions déterminées pour rendre des services à un utilisateur[G] [EB-G].

SIP Session initiation protocol
Protocole de signalisation initialement décrit dans [RFC2543] puis [RFC3261].

SMTP Simple Mail Transport Protocol.

SOF Strength Of Function
Caractéristique d'une SF de la TOE exprimant les efforts minimum supposés nécessaires pour mettre en défaut le comportement de sécurité attendu par attaque directe des mécanismes de sécurité sous-jacents [CC-1].

Sujet (d'un SI)
Entité active d'un SI (les utilisateurs[G] sont des sujets[G]). Les sujets[G] d'un SI manipulent (création, modification, consultation, suppression) les objets[G] du SI. Selon cette définition, un objet[G] peut également agir en tant que sujet[G].

SLA Service Level Agreement
Accord par lequel un fournisseur s'engage à respecter un niveau de service garanti.

SNAT Source Natting
Modification de l'adresse source de datagrammes IP (parfois appelée mascarade).

SNMP Simple Network Management Protocol
Protocole permettant la gestion d'objets réseaux définis dans une base MIB. La version 2 de SNMP (SNMPv2) est notamment décrite dans [RFC3416].

SC Système-Cible
Système composé d'éléments matériels et logiciels faisant l'objet d'un projet de développement ou de déployement.

SI Système d'Information
Ensemble des logiciels, matériels et procédures permettant la gestion des informations au sein d'une entreprise

SSL Secure Socket Layer
Ancien nom du protocole TLS.

ST Security Target
Ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une TOE identifiée [CC-1].

Streaming
Mode de fonctionnement d'applications réseau dans lequel le récepteur traite les informations reçues en temps réel, sans attendre la fin de la communication et sans avoir besoin de connaître a priori la quantité d'informations à recevoir.

TCP Transmission Control Protocol
Protocole de communication (OSI niveau 4, TCP/IP niveau 3) initialement décrit dans [RFC793], puis amendé par [RFC1106], [RFC1122] et [RFC1323].

Telnet
Protocole d'émulation de terminal [RFC764].

TLS Transport Layer Security
Anciennement SSL (développé par Netscape), TLS est un protocole de sécurité permettant l'authentification mutuelle et le chiffrement au niveau de la couche transport des modèles OSI et TCP/IP.

TOE Target Of Evaluation
Produit ou système IT et documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation [CC-1].

TSC TSF Scope of Control
Ensemble des interactions qui peuvent survenir avec ou à l'intérieur d'une TOE et qui sont soumises aux règles édictées par la TSP [CC-1].

TSF TOE Security Functions
Ensemble constitué par tous les éléments matériels, logiciels et programmés de la TOE sur lequel on doit s'appuyer pour l'application correcte de la TSP [CC-1].

TSFI TSF Interface
Ensemble des interfaces, interactives ou programmatiques, par lesquelles on accède aux ressources de la TOE au travers de la TSF, ou par lesquelles on obtient des informations de la TSF [CC-1].

TSP TOE Security Policy
Ensemble de règles qui précisent comment gérer, protéger et distribuer les biens à l'intérieur d'une TOE [CC-1].

TTL Time To Live.

UDP User Datagram Protocol.
Protocole de communication (OSI niveau 4, TCP/IP niveau 3) initialement décrit dans [RFC768].

UML Unified Modeling Language.

Unicast (IP unicast)
Type de communication monodestinataire.

URI Unique Ressource Identifier [RFC2396].

Utilité
Propriété d'un service ou d'une information, fourni par un SI[G], qui est conforme aux besoins et attentes des utilisateurs[G].

Utilisateur

Toute entité (utilisateur humain ou entité IT externe) hors de la TOE et interagissant avec lui [CC-1]. Cette définition est commune à l'UML et aux CC.

Vulnérabilité

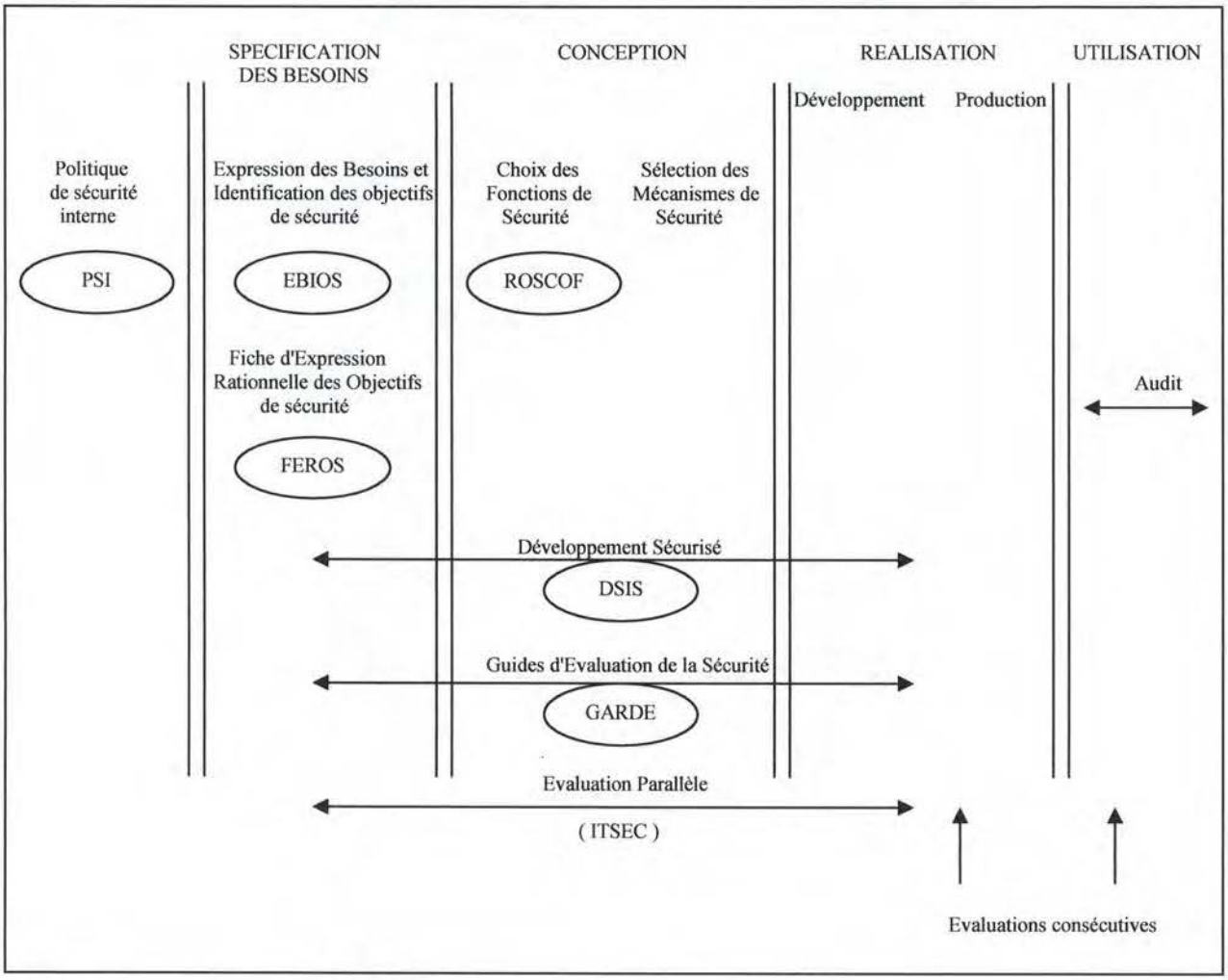
Faiblesse ou faille de sécurité d'un système.

VPN Virtual Private Network

WAN Wide Area Network

Annexes

ANNEXE 1 - Construction de la sécurité d'un système d'information



Source [EB-G]

Légende

	Méthodologie SCSSI
DSIS	Développement de Systèmes d'Information Sécurisés (SCSSI)
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité (SCSSI)
FEROS	Fiche d'Expression Rationnelle des Objectifs de Sécurité (SCSSI)
GARDE	
ITSEC	Information Technology Security Evaluation Criteria [ITSEC]
PSI	Politique de Sécurité Interne (SCSSI)
ROSCOF	Réalisation des Objectifs de Sécurité par le ChOix des Fonctions (SCSSI)
SCSSI	Service Central de la Sécurité des Systèmes d'Information (http://www.ssi.gouv.fr)

Le modèle de cycle de vie utilisé est un cycle de vie simplifié de type ITSEC.

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS)

Tableau A2.1	**Fiche d'expression des besoins de sécurité pour les fonctions**							
Fonction: F_COMM		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Interruption complète (longue durée) de la fonction	2	2	2 (5.3.3.c)	2 (5.3.3.c)	0	2	Voir [1].
	Interruption complète (courte durée) de la fonction	0	0	2	2	0	2	Evaluations transposées (5.3.3.a) du tableau 4.1. Voir [2].
	Dégradation persistante des performances	2	2	2 (5.3.3.c)	2 (5.3.3.c)	0	2	Gêne probable[3]. Voir [4].
Imputabilité	Usurpation de l'identité d'un utilisateur	0	2[5]	3 [6 7 8]	2 [9]	2[10]	3	Voir [11].
Ecologie	Incompatibilité entre applications (erreur de modification de configuration)	0	0	0	0	4 (4.6.5.b)	4	Evaluations transposées (5.3.3.a) des tableaux 4.4 et 4.5.
	Saturation des ressources	0	0	2 (4.6.5.f) (4.6.5.h)	2 (4.6.5.f) (4.6.5.h)	3 (4.6.5.f) (4.6.5.g)	3	Evaluations transposées (5.3.3.a) des tableaux 4.4 et 4.5.

[1] N'entraînerait pas des *pertes financières* au sens du tableau 5.8, mais plutôt un *manque à économiser*.
[2] N'entraînerait pas des *pertes financières* au sens du tableau 5.8, mais plutôt un *manque à économiser*.
[3] Une dégradation des performances d'une communication en streaming est assimilée ici à une indisponibilité complète de longue durée (5.3.3.e).
[4] N'entraînerait pas des *pertes financières* au sens du tableau 5.8, mais plutôt un *manque à économiser*.
[5] Risque de perte en disponibilité (utilisation abusive à l'encontre d'un autre utilisateur (4.5.2.b)); la valeur de l'impact est transposée du tableau 4.3.
[6] Perte en disponibilité pour l'utilisateur légitime (4.5.2.a), assimilée ici à ine interruption complète de courte durée (5.3.3.d).
[7] Risque de perte en disponibilité (utilisation abusive à l'encontre d'un autre utilisateur (4.5.2.b)); la valeur de l'impact est transposée du tableau 4.3.
[8] Risque de submergement des ressources de l'entreprise (multiplication de requêtes fictives (4.5.2.d)); la valeur de l'impact est transposée du tableau 4.3.
[9] Risque de perte en confidentialité quant à l'identité des clients (4.5.2.c); la valeur de l'impact est transposée du tableau 4.3.
[10] Risque de submergement des ressources de l'entreprise (multiplication de requêtes fictives (4.5.2.d)); la valeur de l'impact est transposée du tableau 4.3.
[11] Tenant compte du fait qu'à l'avenir les utilisateurs ne seront probablement pas tous sensés se connaître (4.5.1).

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.2	**Fiche d'expression des besoins de sécurité pour les fonctions**							
Fonction: F_ENROL		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Interruption complète (longue durée) de la fonction	0	1	1	1	0	1	Gêne possible [12] [13] [14].
	Interruption complète (courte durée) de la fonction	0	0	0	0	0	0	Sans impact réel [15] [16].
	Dégradation persistante des performances	0	0	0	0	0	0	Sans impact réel [17] [18].
Imputabilité	Usurpation de l'identité d'un utilisateur	0	2	3	2	2	3	Voir [19].
Ecologie	Incompatibilité entre applications (erreur de modification de configuration)	0	0	2	2	0	2	Valeurs transposées (5.3.3.a) du tableau 4.1 [20].
	Saturation des ressources	0	0	2	2	0	2	Valeurs transposées (5.3.3.a) du tableau 4.1 [21].

[12] Cette opération n'est à effectuer qu'une seule fois pour chaque utilisateur.
[13] L'impact du sinistre ne produit ses effets que vis-à-vis des nouveaux utilisateurs (pas encore enrôlés).
[14] La *gêne possible* est motivée par le délai d'attente.
[15] Cette opération n'est à effectuer qu'une seule fois pour chaque utilisateur.
[16] L'impact du sinistre ne produit ses effets que vis-à-vis des nouveaux utilisateurs (pas encore enrôlés).
[17] Cette opération n'est à effectuer qu'une seule fois pour chaque utilisateur.
[18] L'impact du sinistre ne produit ses effets que vis-à-vis des nouveaux utilisateurs (pas encore enrôlés).
[19] Qu'il s'agisse de l'identité de l'administrateur responsable de l'enrôlement ou de celle d'un autre utilisateur à enrôler, la conséquence sera un impact en imputabilité sur F_COMM (tableau A2.1) et confidentialité sur I_PROFIL (tableau A2.6).
[20] Si la fonction F_ENROL devait s'avérer incompatible avec une autre fonction ou application et la perturber, l'impact se ferait probablement en disponibilité de F_COMM (5.2.4.2.b).
[21] Si la fonction F_ENROL devait s'avérer excessivement consommatrice de ressources au point de perturner une autre fonction ou application, l'impact se ferait probablement en disponibilité sur F_COMM (5.2.4.2.b).

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.3	**Fiche d'expression des besoins de sécurité pour les fonctions**							
Fonction: F_DEVEL		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Interruption complète (longue durée) de la fonction	1	1	1	1[22]	0	1	Gêne possible [23].
	Interruption complète (courte durée) de la fonction	0	0	0	0	0	0	Sans impact réel.
	Dégradation persistante des performances	0	0	0	0	0	0	Sans impact réel.
Imputabilité	Usurpation de l'identité d'un développeur	2	2	3	2	3	3	Evaluations transposées (5.3.3.a) du tableau 4.6. Voir [24].
Ecologie	Incompatibilité entre applications (erreur de modification de configuration)	0	0	2	2	0	2	Evaluations transposées (5.3.3.a) des tableaux 4.4 et 4.5 [25].
	Saturation des ressources	0	0	2	2	0	2	Evaluations transposées (5.3.3.a) des tableaux 4.4 et 4.5 [26].

[22] Dans le cas où une opération importante de maintenance (corrective ou évolutive) serait attendue.
[23] La *gêne possible* est motivée par le délai d'attente.
[24] L'usurpation d'identité d'un utilisateur - ici un développeur - pourrait avoir des conséquences en intégrité sur I_CODSRC.
[25] Si la fonction F_DEVEL devait s'avérer incompatible avec une autre fonction ou application et la perturber, l'impact se ferait probablement en disponibilité au niveau de l'activité normale de l'entreprise, donc aussi sur notre application (4.6.5.i). Rappelons que EBIOS préconise l'évaluation de l'impact potentiel indépendamment de la probabilité du sinistre (5.3.3.b) (dans ce cas particuler, nous avions estimé la menace nulle (4.6.5.d)).
[26] Si la fonction F_DEVEL devait s'avérer excessivement consommatrice de ressources au point de perturner une autre fonction ou application, l'impact se ferait probablement en disponibilité au niveau de l'activité normale de l'entreprise, donc aussi sur notre application (4.6.5.i).

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.4	**Fiche d'expression des besoins de sécurité pour les fonctions**							
Fonction: F_DEPLO		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Interruption complète (longue durée) de la fonction	1	1	1	1[27]	0	1	Gêne possible[28].
	Interruption complète (courte durée) de la fonction	0	0	0	0	0	0	Sans impact réel.
	Dégradation persistante des performances	0	0	0	0	0	0	Sans impact réel.
Imputabilité	Usurpation de l'identité d'un administrateur	0	0	0	0	0	0	Voir[29].
Ecologie	Incompatibilité entre applications (erreur de modification de configuration)	0	0	0	0	4 (4.6.5.b)	4	Evaluations transposées (5.3.3.a) des tableaux 4.4 et 4.5[30].
	Saturation des ressources	0	0	2 (4.6.5.f) (4.6.5.h)	2 (4.6.5.f) (4.6.5.h)	3 (4.6.5.f) (4.6.5.g)	3	Evaluations transposées (5.3.3.a) des tableaux 4.4 et 4.5[31].

[27] Dans le cas où une opération importante de maintenance (corrective ou évolutive) serait attendue.
[28] La *gêne possible* est motivée par le délai d'attente.
[29] L'usurpation d'identité d'un utilisateur - ici le responsable du déploiement - n'aurait aucun effet réel selon l'hypothèse de base que F_DEPLO ne permet de déployer que du code dûment validé (5.3.3.k).
[30] Si la fonction F_DEPLO devait s'avérer incompatible avec une autre fonction ou application et la perturber, l'impact le plus important se ferait probablement en disponibilité au niveau des activités stratégiques (mais également au niveau des activités normales de l'entreprise, donc aussi sur notre application (4.6.5.i)).
[31] Si la fonction F_DEPLO devait s'avérer excessivement consommatrice de ressources au point de perturber une autre fonction ou application, l'impact se ferait probablement en disponibilité au niveau de des activités stratégiques (mais également au niveau des activités normales de l'entreprise, donc aussi sur notre application (4.6.5.i)).

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.5	**Fiche d'expression des besoins de sécurité pour les informations**							
Type: I_AUTH		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Perte totale (destruction) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM[32].
	Perte temporaire (inaccessibilité) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM.
Confidentialité	Divulgation interne	0	0	0	0	0	0	Sans impact réel.
	Divulgation externe	0	2	3	2	2	3	Permet l'usurpation d'identité. Evaluations transposées (5.3.3.a) du tableau 4.3.
Imputabilité	Usurpation des privilèges de l'administrateur	0	2	3	2	2	3	Permet l'usurpation d'identité. Evaluations transposées (5.3.3.a) du tableau 4.3 [33].
Intégrité	Modification accidentelle	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM.
	Modification délibérée	0	2	3	2	2	3	Permet l'usurpation d'identité. Evaluations transposées (5.3.3.a) du tableau 4.3 [34].

[32] L'information peut être remplacée aisément en procédant à nouveau à l'enrôlement des utilisateurs.
[33] Rend également possible l'indisponibilité totale temporaire, dont les valeurs d'impact sont inférieures ou égales à celles encourues en cas d'usurpation d'identité..
[34] Rend également possible l'indisponibilité totale temporaire, dont les valeurs d'impact sont inférieures ou égales à celles encourues en cas d'usurpation d'identité..

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.6	**Fiche d'expression des besoins de sécurité pour les informations**							
Type: I_PROFIL		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Perte totale (destruction) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM [35].
	Perte temporaire (inaccessibilité) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM.
Confidentialité	Divulgation interne	0	0	0	0	0	0	Sans impact réel.
	Divulgation externe	0	0	0	2 (4.4.2.d)	0	2	Confidentialité des profils utilisateurs (4.4.1.e).
Imputabilité	Usurpation des privilèges de l'administrateur	0	0	2 (4.7.2.i)	2 (4.7.2.h)	0	2	Intégrité des profils utilisateurs (4.7.2.h) [36].
Intégrité	Modification accidentelle	0	0	2 (4.7.2.i)	2 (4.7.2.h)	0	2	Intégrité des profils utilisateurs (4.7.2.h) [37].
	Modification délibérée	0	0	2 (4.7.2.i)	2 (4.7.2.h)	0	2	Intégrité des profils utilisateurs (4.7.2.h) [38].

[35] L'information peut être remplacée aisément en procédant à nouveau à l'enrôlement des utilisateurs.
[36] L'usurpation de l'identité de l'administrateur permet une atteinte à l'intégrité des profils des utilisateurs, d'où impact également en disponibilité (4.7.2.i).
[37] D'où impact également en disponibilité (4.7.2.i) (comportement "opportuniste" de l'utilisateur).
[38] D'où impact également en disponibilité (4.7.2.i).

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.7	**Fiche d'expression des besoins de sécurité pour les informations**							
Type: I_COMM		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Perte totale (destruction) de l'information	0	0	2	2	0	2	Indisponibilité temporaire de F_COMM (tableau A1.1)
	Perte temporaire (inaccessibilité) de l'information	0	0	2	2	0	2	Indisponibilité temporaire de F_COMM (tableau A1.1)
Confidentialité	Divulgation interne	0	2 (4.4.2.g)	0	0	0	2	Evaluations transposées (5.3.3.a) du tableau 4.2.
	Divulgation externe	1	2 (4.4.2.g)	2 (4.4.2.f)	2 (4.4.2.e)	3 (4.4.2.e)	3	Evaluations majoritairement transposées (5.3.3.a) du tableau 4.2.
Imputabilité	Usurpation de l'identité d'un utilisateur	0	2	3	2	2	3	Voir [39].
Intégrité	Modification accidentelle	0	0	2	2	0	2	Atteinte en disponibilité[G] (4.7.2.j).
	Modification délibérée	0	0	2	2	0	2	Atteinte en disponibilité[G] (4.7.2.j).

[39] Assimilé au risque correspondant encouru par la fonction F_COMM (tableau A2.1).

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.8	**Fiche d'expression des besoins de sécurité pour les informations**							
Type: I_CODSRC		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Perte totale (destruction) de l'information	2	2	2	2	0	2	Voir [40].
	Perte temporaire (inaccessibilité) de l'information	0	0	0	0	0	0	Sans impact réel [41].
Confidentialité	Divulgation interne	0	0	0	0	0	0	Sans impact réel (4.4.2.c).
	Divulgation externe	0	0	0	0	0	0	Sans impact réel (4.4.2.c).
Imputabilité	Usurpation des privilèges d'un développeur	2	2	3	2	3	3	Evaluations transposées (5.3.3.a) du tableau 4.6. Voir [42].
Intégrité	Modification accidentelle	2	2	3	2	3	3	Evaluations transposées (5.3.3.a) du tableau 4.6.
	Modification délibérée	2	2	3	2	3	3	Evaluations transposées (5.3.3.a) du tableau 4.6.

[40] Selon le cas pire: perte des sources d'une application développée, d'où impossibilité d'en assurer la maintenance (surtout corrective): à terme, risque de perte totale en disponibilité de l'application (interruption complète de longue durée de F_COMM, tableau A2.1)
[41] Equivaut à une indisponibilité complète de courte durée de la fonction F_DEVEL (tableau A2.3).
[42] L'usurpation d'identité d'un utilisateur - ici un développeur - pourrait avoir des conséquences en intégrité sur I_CODSRC.

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.9	**Fiche d'expression des besoins de sécurité pour les informations**							
Type: I_CODBIN		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Perte totale (destruction) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM [43].
	Perte temporaire (inaccessibilité) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM [44].
Confidentialité	Divulgation interne	0	0	0	0	0	0	Sans impact réel.
	Divulgation externe	0	0	0	0	0	0	Sans impact réel.
Imputabilité	Usurpation des privilèges de l'administrateur	0	0	2	2	0	2	Voir [45].
Intégrité	Modification accidentelle	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM [46].
	Modification délibérée	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM [47].

[43] Le temps de regénérer et/ou redéployer.
[44] Le temps de regénérer et/ou redéployer.
[45] Permet une atteinte à la disponibilité du code.
[46] Le temps de regénérer et/ou redéployer.
[47] Le temps de regénérer et/ou redéployer.

ANNEXE 2 - Fiches d'expression des besoins de sécurité (EBIOS) (suite)

Tableau A2.10	**Fiche d'expression des besoins de sécurité pour les informations**							
Type: I_PARAM		*Impacts*						
Critères	*Sinistres*	*Réduction des coûts*	*Recherche de synergies*	*Amélioration du support*	*Image de l'entreprise*	*Objectifs stratégiques*	*MAX*	*Commentaires*
Disponibilité	Perte totale (destruction) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM [48].
	Perte temporaire (inaccessibilité) de l'information	0	0	2	2	0	2	Equivaut à une indisponibilité totale temporaire de F_COMM [49].
Confidentialité	Divulgation interne	0	0	0	0	0	0	Sans impact réel [50].
	Divulgation externe	0	0	0	0	0	0	Sans impact réel [51].
Imputabilité	Usurpation des privilèges de l'administrateur	0	0	2	2	3	3	Permet la modification délibérée (ci-dessous)..
Intégrité	Modification accidentelle	0	0	2	2	3	3	Peut mener à une atteinte à l'écologie des fonctions (saturation de ressources).
	Modification délibérée	0	0	2	2	3	3	Peut mener à une atteinte à l'écologie des fonctions (saturation de ressources).

[48] Le temps de reconstituer l'information.
[49] Le temps de retrouver l'information.
[50] Sous réserve de la nature exacte des informations de configuration (à ce stade sont considérés (4.3.3.g) (4.3.3.h)).
[51] Sous réserve de la nature exacte des informations de configuration (à ce stade sont considérés (4.3.3.g) (4.3.3.h)).

ANNEXE 3 - Pertes financières par type d'impact [CLUSIF19]

Tableau A3.1	**Pertes financières (exprimées en 10^6 FF) ventilées par type de menace et résultant d'un impact en disponibilité. Rapports du CLUSIF, 1991 à 1996 [CLUSIF19]**													
	Rapport 1991		*Rapport 1992*		*Rapport 1993*		*Rapport 1994*		*Rapport 1995*		*Rapport 1996*		*TOTAUX*[52]	
Type de menace	*Pertes*	*%1991*	*Pertes*	*%1992*	*Pertes*	*%1993*	*Pertes*	*%1994*	*Pertes*	*%1995*	*Pertes*	*%1996*	*Pertes*	*%*
A1	1000	22,57	1020	22,87	1090	24,36	1130	24,35	1170	24,71	1450	28,10		
A2	800	18,06	750	16,82	750	16,76	60	16,38	760	16,05	860	16,67		
A3	70	1,58	90	2,02	110	2,46	110	2,37	100	2,11	35	0,68		
A4	240	5,42	220	4,93	225	5,03	250	5,39	260	5,49	260	5,04		
A5	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
E1	300	6,77	300	6,73	260	5,81	200	4,31	150	3,17	100	1,94		
E2	400	9,03	430	9,64	430	9,61	410	8,84	430	9,08	400	7,75		
M1	60	1,35	80	1,79	0	0,00	70	3,66	190	4,01	230	4,46		
M2	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	200	3,88		
M3	10	0,23	0	0,00	0	0,00	0	0,00	0	0,00	5	0,10		
M4	400	9,03	420	9,42	440	9,83	440	9,48	445	9,40	270	5,23		
M5	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
M6	1150	25,96	1150	25,78	1170	26,15	1170	25,22	1230	25,98	1350	26,16		
TOTAUX[53]	4430	00,00	4460	100,00	4475	100,00	4640	100,00	4735	100,00	5160	100,00		
PERCENTILES[54]		84,65		84,53		86,70		84,27		85,22		83,91		

[52] Totaux par type de menace
[53] Totaux par période.
[54] Pourcentage de la contribution des champs en léger grisé dans le total

ANNEXE 3 - Pertes financières par type d'impact [CLUSIF19] (suite)

Tableau A3.2	**Pertes financières (exprimées en 10^6 FF) ventilées par type de menace et résultant d'un impact en confidentialité. Rapports du CLUSIF, 1991 à 1996 [CLUSIF19]**													
	Rapport 1991		*Rapport 1992*		*Rapport 1993*		*Rapport 1994*		*Rapport 1995*		*Rapport 1996*		*TOTAUX*[55]	
Type de menace	*Pertes*	*%1991*	*Pertes*	*%1992*	*Pertes*	*%1993*	*Pertes*	*%1994*	*Pertes*	*%1995*	*Pertes*	*%1996*	*Pertes*	*%*
A1	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
A2	10	0,48	10	0,46	10	0,45	10	0,40	10	0,38	0	0,00		
A3	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
A4	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
A5	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
E1	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
E2	20	0,96	20	0,91	20	0,89	20	0,80	20	0,77	20	0,69		
M1	10	0,48	10	0,46	0	0,00	0	0,00	10	0,38	10	0,35		
M2	50	2,39	50	2,28	0	0,00	0	0,00	0	0,00	0	0,00		
M3	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
M4	50	2,39	50	0,28	65	2,90	65	2,62	65	2,50	0	0,00		
M5	700	33,49	770	35,16	820	36,53	860	34,61	900	34,55	1100	38,06		
M6	1250	59,81	1280	58,45	1330	59,24	1530	61,57	1600	61,42	1760	60,90		
TOTAUX[56]	2090	100,00	2190	100,00	2245	100,00		100,00	2605	100,00	2890	100,00		
PERCENTILES[57]		93,30		93,61		97,77	2485	96,18		95,97		98,96		

[55] Totaux par type de menace
[56] Totaux par période.
[57] Pourcentage de la contribution des champs en léger grisé dans le total

ANNEXE 3 - Pertes financières par type d'impact [CLUSIF19] (suite)

Tableau A3.3	**Pertes financières (exprimées en 10^6 FF) ventilées par type de menace et résultant d'un impact en intégrité et imputabilité. Rapports du CLUSIF, 1991 à 1996 [CLUSIF19]**													
	Rapport 1991		*Rapport 1992*		*Rapport 1993*		*Rapport 1994*		*Rapport 1995*		*Rapport 1996*		*TOTAUX*[58]	
Type de menace	*Pertes*	*%1991*	*Pertes*	*%1992*	*Pertes*	*%1993*	*Pertes*	*%1994*	*Pertes*	*%1995*	*Pertes*	*%1996*	*Pertes*	*%*
A1	300	7,81	300	7,92	300	7,33	300	7,36	300	7,11	180	3,85		
A2	190	4,95	190	5,01	200	4,89	200	4,91	260	6,16	250	5,35		
A3	30	0,78	30	0,79	30	0,73	30	0,74	0	0,00	0	0,00		
A4	10	0,26	10	0,26	10	0,24	10	0,25	10	0,24	20	0,43		
A5	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
E1	580	15,10	640	16,89	640	15,65	700	17,18	700	16,59	700	14,99		
E2	500	13,02	510	13,46	520	12,71	520	12,76	550	13,03	600	12,85		
M1	30	0,78	30	0,79	140	3,42	0	0,00	0	0,00	0	0,00		
M2	1700	44,27	1500	39,58	1630	39,85	1620	39,75	1670	39,57	2100	44,97		
M3	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
M4	500	13,02	580	15,30	620	15,16	695	17,06	730	17,30	820	17,56		
M5	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
M6	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00	0	0,00		
TOTAUX[59]	3840	100,00	3790	100,00	4090	100,00	4075	100,00	4220	100,00	4670	100,00		
PERCENTILES[60]		85,42		85,22		83,37		86,75		86,49		90,36		

[58] Totaux par type de menace
[59] Totaux par période.
[60] Pourcentage de la contribution des champs en léger grisé dans le total

ANNEXE 4 - Description de la grille harmonisée des menaces informatiques [CEA]

Reproduction avec l'aimable autorisation du CEA.

Tableau A4.1	**Grille harmonisée des menaces informatiques**					
Types de conséquences:	*Conséquences financières directes*		*Conséquences financières indirectes*			
Types de menaces	*C1*	*C2*	*C3*	*C4*	*C5*	*C6*
Catégorie 'A' - Accidents						
A1 Physiques						
A2 Pannes						
A3 Evénements naturels						
A4 Perte de services						
A5 Autres						
Catégorie 'E' - Erreurs						
E1 Erreurs d'utilisation						
E2 Erreurs de conception						
Catégorie 'M' - Malveillance						
M1 Vol						
M2 Fraude						
M3 Sabotage						
M4 Attaque logique						
M5 Divulgation						

TYPES DE RISQUES

ACCIDENTS

- **A1** Incendie, explosion, implosion
- **A2** Pannes (matérielles et logiques) : il s'agit de l'ensemble des causes d'origine ou de révélation interne entraînant l'indisponibilité ou le dysfonctionnement (non conformité aux fonctionnalités et performances nominales) total ou partiel du système.
- **A3** Evénements naturels : il s'agit des événements naturels d'origine externe au système : inondation, tempête, cyclone, ouragan, vent, poids de la neige sur les toitures, foudre, grêle, avalanche, coulée de boue, glissement de terrain, phénomènes sismiques et volcaniques, etc.
- **A4** Perte de services essentiels : il s'ait de l'ensemble des causes d'origine externe entraînant l'indisponibilité ou le dysfonctionnement (non conformité au fonctionnalités et performances nominales) total ou partiel du système :
  - électricité, télécommunications, eau
  - fluides divers
  - fournitures spécifiques (rupture de stock papier...)
- **A5** Autres risques accidents physiques: il s'agit de l'ensemble des causes d'origine interne ou externe au système endommagé qui ont conduit à son endommagement accidentel total ou partiel:
  - chocs, collisions, chutes
  - introduction de corps étrangers solides, liquides, gazeux ou mixtes, ayant des actions physiques ou chimiques (y compris la pollution)
  - bris de machine accidentels de type mécanique, électrique, électronique, électromagnétique
  - pollution par rayonnement (thermique, électromagnétique, nucléaire, etc.), effets électrostatiques, etc.

ERREURS

- **E1** Erreurs d'utilisation (logique) : erreurs de saisie et transmission des données quel qu'en soit le moyen, erreurs d'exploitation du système.
- **E2** Erreurs de conception et de réalisation de logiciels et procédures d'application.

ANNEXE 4 - Description de la grille harmonisée des menaces informatiques [CEA] (suite)

MALVEILLANCE

- **M1** Vol
- **M2** Fraude : utilisation non autorisée des ressources du système d'information, conduisant à un préjudice évaluable monétairement pour la victime, essentiellement formé par le détournement de biens au profit du criminel:
  - détournement de fonds
  - détournement de biens ou services (matériels ou immatériels)
- **M3** Sabotage : action malveillante conduisant à un sinistre matériel (type A1 ou A2).
- **M4** Attaque logique : utilisation non autorisée des ressources du système d'information, conduisant à un préjudice au moins qualitatif pour la victime, se traduisant essentiellement par une perte d'intégrité et/ou de disponibilité, entraînant le plus souvent un profit indirect pour le criminel et/ou le commanditaire éventuel.
- **M5** Divulgation : utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles.
- **M6** Autres

CONSEQUENCES FINANCIERES

DIRECTES

- **C1** (Matériels): frais d'expertise, de déblaiement, de réparation ou de remplacement des matériels endommagés.
- **C2** (Non matériels): frais d'expertise et de restauration des éléments non-matériels du système atteint : système d'exploitation, données, programmes, procédures, documentations et divers.

N.B: tous les frais de reconstitution, quelle que soit son ampleur (liée par exemple à l'insuffisance de sauvegardes), sont conventionnellement comptabilisés en C2.

INDIRECTES

- **C3** (Frais supplémentaires)
  - Frais supplémentaires: ensemble des frais correspondant à des mesures conservatoires destinées à maintenir pour le système des fonctionnalités et performances aussi proche que possible de celles qui étaient les siennes avant le sinistre jusqu'à remise en état (matériel et non- matériel).
  - Pertes d'exploitation : pertes de marge dues à des frais supplémentaires et/ou à des pertes de revenus directes ou indirectes (pertes d'affaires,de clients, d'image, etc.).
- **C4** (Pertes de fonds et de biens):
  - pertes de fonds ou de biens physiques
  - pertes d'informations confidentielles, de savoir-faire, etc.
  - pertes d'éléments non reconstituables du système (essentiellement données ou programmes) évalués en valeur patrimoniale.
- **C5** (Responsabilité civile): responsabilité civile encourue par l'entreprise ou l'organisme du fait des préjudices causés à autrui, volontairement ou pas, du fait de la survenance d'un sinistre dans son enceinte juridique.
- **C6** (Autres pertes): qualitatives, réglementaires, déontologiques, etc.

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA]

Tableau A5.1	**La fiche de recommandation 1.**											
*	*Education*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	La direction générale doit avoir été sensibilisée aux risques informatiques et à la politique de sécurité qui doit être mise en œuvre en corollaire. Cette sensibilisation est formalisée par une réunion de l'ordre de deux heures où un spécialiste expose les faits sur la base d'exemples concrets de sinistres (en insistant sur les aspects organisationnels, la situation de crise et les conséquences) , puis la stratégie de management du risque en trois phases, l'organisation et les structures, puis les coûts.											
R2	L'encadrement doit recevoir une sensibilisation de même type que la direction générale et, en plus, une initiation à la sécurité (1 à 3 jours) : management, conduite et contrôle de projets, produits et service de sécurité, règles de sécurité. Certains techniciens de l'informatique et les agents de sécurité informatique doivent recevoir une formation spécialisée approfondie(5 à 20 jours).											
R3	L'ensemble du personnel doit être régulièrement sensibilisé (1 heure). Cela peut se faire par petits groupes homogènes, sur la base de cas concrets(risques/- mesures) concernant directement ces agents. Ceci peut être renforcé par la diffusion de supports (plaquettes, ,affichettes, , autocollants, ,pins, films vidéo, manuels de sécurité, etc.).											
Commentaire	La sécurité repose d'abord sur les hommes (qui génèrent ou conditionnent un grand nombre de sinistres, jouent un rôle dans la situation de crise et tout le processus de sécurité : conception et mise en œuvre, puis la protection et naturellement la dissuasion). La formation doit être adaptée, avec des rappels périodiques. C'est elle qui conditionne très largement l'efficacité du dispositif de sécurité (sinon il y aura méfiance, contre passage des mesures, inadéquation des procédures, dérives diverses, etc.).											

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Reproduction avec l'aimable autorisation du CEA.

Tableau A5.2	**La fiche de recommandation 4.**											
*	*Classification des objets*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	On doit recenser les objets (données, procédures) informatiques ou non informatiques considérés comme essentiels, et désigner des propriétaires fonctionnels de ces objets. Ceux-ci devront mettre en œuvre les procédures de sécurité concernant les objets qui s'imposeront à tous les personnels les utilisant.											
R2	On procédera à une classification rigoureuse des objets. Celle-ci repose sur l'analyse des risques appliquée à chaque objet conduisant à la connaissance des menaces spécifiques et à l'évaluation de la gravité des connaissances en disponibilité (D) , intégrité (I) , confidentialité ©. Chaque objet reçoit ainsi une étiquette DIC qui caractérise sa valeur . Ces étiquettes sont gérées dans le dictionnaire de l'entreprise. Dès qu'une procédure concerne un objet, on vérifie que les mesures de sécurité sont en rapport avec la valeur de l'objet et l'on agit en conséquence. On procédera à une classification des sujets selon des critères spécifiques et, avec l'aide des propriétaires des objets et du responsable sécurité, on croisera les classifications objets/sujets pour aboutir aux règles formelles des droits d'accès des sujets aux objets. Ces procédures seront régulièrement adaptées, mises à jour et contrôlées. Chaque changement (sujet ou objet) doit entraîner une mise à jour immédiate.											
R3	On utilisera systématiquement et formellement les étiquettes DIC pour la conception des systèmes d'information, notamment en ce qui concerne le développement d'applications informatiques et les systèmes de contrôle d'accès logiques. On tiendra compte des relations entre les objets afin de contrôler la cohérence des classifications et des droits d'accès.											
Commentaire	La connaissance des objets en nature et en valeur est le fondement de très nombreuses action de sécurité . Celle-ci doit en effet être discriminante et adaptée à cette valeur selon les menaces attendues. Chacun sait par exemple qu'un progiciel de contrôle d'accès n'a pas d'efficacité réelles si les droits d'accès ne sont pas basés sur une telle étude. Ou encore que les contrôles programmés dans les applications informatiques sont hélas trop souvent sans rapport avec les véritables risques et enjeux.											

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Tableau A5.3	**La fiche de recommandation 5.**											
**	*Analyse des risques*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	L'entreprise doit être dotée d'un plan de sécurité justifié, c'est-à-dire reposant sur une analyse chiffrée et discriminante des risques. Ce plan doit prévoir les actions, notamment celles prioritaires, dans leur contenu technique et organisationnel, ainsi que les coûts et structures nécessaires.											
R2	L'approche doit reposer sur une méthode formelle reconnue (MARION, CRAMM, etc.). Les objectifs de la direction générale doivent être formalisés et interprétés en indicateurs objectifs qui serviront à valoriser les scénarios de menaces possibles (en gravité, c'est-à-dire en tenant compte de l'impact maximum possible et de la possibilité de réalisation).											
R3												
Commentaire	Le plan (ou schéma direction) sécurité des systèmes d'information est le point de départ logique de toute démarche : - c'est lui qui convainc les décideurs d'agir à partir du bilan entre les menaces et les coûts de sécurité ; - c'est lui qui définit les priorités et l'organisation. C'est donc lui qui garantit la cohérence et l'adéquation des solutions, ce qui est un des aspects fondamentaux de la sécurité (bien souvent la sécurité est envisagée au coup par coup, en fonction des incidents, des évidences ou des a priori. On sait qu'en pratique, cela n'empêche pas les sinistres et en particulier les grands sinistres).											

Tableau A5.4	**La fiche de recommandation 6**											
**	*Procédures de sécurité*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	Les solutions résultant du plan de sécurité doivent toujours être accompagnées de procédures formalisées par écrit. Celles-ci doivent être correctement et régulièrement diffusées et mises à jour. Les personnels concernés doivent être régulièrement informés et formés au plan général (évolution des risques et des techniques, état d'avancement des réalisations de sécurité, etc.) et au plan spécifique (mesures techniques et procédures de sécurité les concernant directement).											
R2												
R3												
Commentaire	Ces mesures viennent en complément de l'éducation générale . Les solutions ne sont efficaces que si les personnels sont compétents.											

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Reproduction avec l'aimable autorisation du CEA.

Tableau A5.5	**La fiche de recommandation 7**
**	*Audit*
Champ	A1 A2 A3 A4 A5 E1 E2 M1 M2 M3 M4 M5
R1	L'encadrement doit appliquer les règles du contrôle interne au processus informatiques. Le responsable sécurité peut aider en ce sens les opérationnels, mais cela reste leur responsabilité normale.
R2	L'audit interne ou externe doit procéder régulièrement et de façon impromptue à un certain nombre de contrôles portant sur les points-clé de la sécurité ainsi que sur les actions essentielles : - classification exhaustive et à jour des objets ; - plan et moyens de secours ; - plan et moyens de sauvegarde ; - sécurité physique de base (incendie, accès) ; - système d'authentification et de contrôle des accès ; - moyens de contrôle d'intégrité et de confidentialité ; - sécurité d u réseau ; - moyens de lutte contre le sabotage immatériel ; - sécurité du développement des applications.
R3	On peut faire appel à un spécialiste pour tenter de « briser « les mesures de sécurité afin d'en vérifier l'efficacité (virus, pénétration du réseau, etc.).
Commentaire	Le bon fonctionnement de la sécurité ne peut être garanti que s'il est contrôlé par des tiers indépendants.

Tableau A5.6	**La fiche de recommandation 9**
**	*Bâtiments (généralités)*
Champ	A1 A2 A3 A4 A5 E1 E2 M1 M2 M3 M4 M5
R1	Les bâtiments abritant l'informatique doivent correspondre à leur destination, vis-à-vis des risques d'incendie, dégâts des eaux, risques électriques, effondrement, etc.
R2	Les bâtiments doivent être compartimentés de façon étanche (vis-à-vis de l'incendie, des fumées de l'eau et surtout des personnes) en fonction de leur classification (contenu et activité) et des contraintes. En ce qui concerne le contrôle d'accès physique, on contrôlera rigoureusement le passage des personnes entre deux compartiments de classes différentes.
R3	
Commentaire	Dans le cas des petites entreprises ou dans l'environnement des petits systèmes, on se fondera sur le compartimentage général et l'on fera en sorte de ne pas disposer les systèmes informatiques dans les locaux dangereux ou vulnérables.

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Tableau A5.7	**La fiche de recommandation 20**											
***	*Authentification et contrôle d'accès logique*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	Il doit exister un système efficace, cohérent et exhaustif (couvrant tous les sous-systèmes) de contrôle d'accès logique au système informatique, utilisant un mode d'identification et d'authentification fiable, fondé sur des droits d'accès spécifiques, justifiés et correctement mis à jour.											
R2	Le système (matériel ou progiciel) de contrôle d'accès logique doit offrir une granularité d'accès (sinon, il faut la compléter, notamment dans les applications informatiques). Il est souhaitable que l'utilisateur définisse lui-même les mots de passe (suffisamment longs, non triviaux conservés confidentiellement, chiffrés en table système) et les change souvent. Les transactions doivent être journalisées (dans un fichier protégé à accès restreint). Le journal d'audit doit être régulièrement analysé.											
R3	On utilisera un système ayant au moins la classe TCSEC/B2 , en étroite liaison avec le système de classification des objets, des sujets et des droits dynamiques sujets/objets.											
Commentaire	Les biens immatériels (données) sont au moins aussi précieux que les biens matériels. Il faut donc en protéger l'accès (lecture, création, suppression, modification) afin d'éviter les ruptures : - de confidentialité (lecture) ; - d'intégrité (notamment par modifications) ; - de disponibilité (notamment par suppressions ou par modifications massives). Le contrôle d'accès repose sur un ensemble de points dont il faut veiller à ce qu'ils soient cohérents : - définition justifiée des droits d'accès (à granularité fine) ; - éducation des personnels concernés ; - procédures rigoureuses de mise à jour ; - système de contrôle d'accès étanche ; - audit régulier. -											

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Reproduction avec l'aimable autorisation du CEA.

Tableau A5.8	**La fiche de recommandation 21**											
*	*Journalisation*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	On conservera (en archivant régulièrement) de façon sécurisée et pendant une période suffisante les enregistrements des transactions (log file). On les analysera régulièrement (dépistage et exploitation en cas d'incident).											
R2												
R3	-											
Commentaire	De nombreuses erreurs ou failles sont souvent liées à des incohérences dans les versions des logiciels exploités.											

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Reproduction avec l'aimable autorisation du CEA.

Tableau A5.9	**La fiche de recommandation 22**											
**	*Sécurité des applications informatiques*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	Les programmes développés en interne doivent comporter des contrôles d'intégrité efficaces, en rapport avec la valeur des informations traitées. Les progiciels achetés à l'extérieur doivent être conforme à la même règle. Pour cela, ils doivent êtres documentés, voire certifiés. L'acheteur doit exprimer formellement ses besoins et tester le produit.											
R2	Pour les logiciels conçus et développés en interne, on doit utiliser une méthodologie ayant les caractéristiques suivantes : - prise en compte de la classification des objets (si possible dans le dictionnaire des données) en ajustant en conséquence le niveau de sécurité ; - définition des mesures de sécurité globales ou relatives à certains groupes d'objets en fonction des classifications ; - vérification a posteriori de l'efficacité des mesures. Pour les progiciels extérieurs, on doit disposer des éléments suivants : - un cahier des charges disposant d'un chapitre formel de sécurité qui fera l'objet de contrôles lors de la réception (entre les études et l'exploitation informatique) ; - une procédure de quarantaine (isolement sur un système spécifique) ; - une procédure d'analyse de conformité; - une procédure de détection d'anomalies ou de séquences anormales ; - une procédure de scellement pour diffusion.											
R3	L'administration des données doit être rigoureuse : - journalisation des modifications des bases de données stratégiques ; - chiffrement des données confidentielles stockées et transmises ; - contrôle d'intégrité régulier des informations stockées et transmises (scellement, parité, ,etc.) ; - procédure de non-répudiation à l'émission et à la réception de messages stratégiques. Les applications informatiques doivent être parfaitement documentées à différents niveaux (fonctionnel et organique) et cette documentation complète et cohérente doit être tenue à jour, ,protégée, sauvegardée. On doit procéder à une recette rigoureuse des applications en exploitation. De même, les progiciels acquis doivent être isolés pour analyse avant d'être diffusés.											
Commentaire	La sécurité des logiciels est l'un des points les plus défaillants que relève généralement un audit. Ceci est dû à la masse, à l'ancienneté, à la complexité, à des délais souvent serrés pour le développement et la maintenance. Pourtant les failles offertes par les logiciels constituent le fondement de nombreuses pertes d'intégrité accidentelles ou malveillantes. Il faut corriger les applications stratégiques et mettre en œuvre dès que possible des méthodes de conception, de développement et de recette assurant le juste niveau de sécurité pour les applications nouvelles et les maintenances lourdes.											

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Tableau A5.10	**La fiche de recommandation 23**											
*	*Documentation*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	Il doit exister une documentation correcte, claire, exhaustive et à jour couvrant : - les matériels, l'architecture ; - les systèmes d'exploitation et logiciels de base ; - le réseau ; - les procédures d'exploitation ; - les applications ; - les fichiers et bases de données stratégiques ; - les procédures de sécurité.											
R2	Cette documentation technique doit être régulièrement sauvegardée et protégée.											
R3												
Commentaire	En cas d'incident d'intégrité, la documentation permet, lorsqu'elle est bien faite, de déterminer et de corriger rapidement les causes. En cas de perte de disponibilité des programmes (sinistre physique total ou sabotage des sources et de leurs sauvegardes), la documentation permet d'accélérer la reconstitution ou de favoriser le choix de solutions de substitution temporaires.											

Tableau A5.11	**La fiche de recommandation 26**											
*	*Accès aux salles informatiques*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	L'accès aux salles informatiques doit être hiérarchisé et strictement réservé à ceux qui ont absolument besoin de s'y rendre.											
R2												
R3												
Commentaire												

ANNEXE 5 - Fiches de recommandations sélectionnées [CEA] (suite)

Reproduction avec l'aimable autorisation du CEA.

Tableau A5.12	**La fiche de recommandation 27**											
**	*Journalisation de la maintenance*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	Les opérations de maintenance (physique et logique) doivent être rigoureusement contrôlées et enregistrées dans un journal.											
R2	On enregistrera notamment la succession des releases, patches et add-on sur le système d'exploitation et les logiciels de base, avec la chronologie et la symptomatique exactes.											
R3	-											
Commentaire	De nombreuses erreurs ou failles sont souvent liées à des incohérences dans les versions des logiciels exploités.											

Tableau A5.13	**La fiche de recommandation 28**											
28	*Sécurité de l'exploitation*											
Champ	A1	A2	A3	A4	A5	E1	E2	M1	M2	M3	M4	M5
R1	- Analyse régulière des comptes rendus d'exploitation - Contrôle des procédures d'exploitation - Analyse des performances - Analyse des anomalies - Suivi qualité - Séparation des objets et ressources d'exploitation de ceux de développement											
R2	- Pistage, traçage des warnings - Mise en œuvre de procédures contre le sabotage immatériel - Contrôle des sources (dates de modification, taille des modules, check-sum, scellés, etc.)											
R3	- Analyse du trafic réseau (interne et externe) - Détection des écoutes - Lutte contre le rayonnement compromettant.											
Commentaire	La surveillance du système permet de détecter des erreurs et surtout des tentatives d'attaques logiques.											

ANNEXE 6 - Répertoire des menaces génériques (EBIOS)

Tableau A6.1	**Menaces génériques EBIOS par thème** Sources: [EB-O]
Thèmes	*Menaces*
I ACCIDENTS PHYSIQUES	**1-** INCENDIE **2-** DÉGÂTS DES EAUX **3-** POLLUTION **4-** ACCIDENTS MAJEURS
II ÉVÉNEMENTS NATURELS	**5-** PHÉNOMÈNE CLIMATIQUE **6-** PHÉNOMÈNE SISMIQUE **7-** PHÉNOMÈNE VOLCANIQUE **8-** PHÉNOMÈNE MÉTÉOROLOGIQUE **9-** CRUE
III PERTE DE SERVICES ESSENTIELS	**10-** DÉFAILLANCE DE LA CLIMATISATION **11-** PERTE D'ALIMENTATION ÉNERGÉTIQUE **12-** PERTE DES MOYENS DE TÉLÉCOMMUNICATIONS
IV PERTURBATIONS DUES AUX RAYONNEMENTS	**13-** RAYONNEMENTS ÉLECTROMAGNÉTIQUES **14-** RAYONNEMENTS THERMIQUES **15-** IMPULSIONS ÉLECTROMAGNÉTIQUES (IEM)
V COMPROMISSION DES INFORMATIONS	**16-** INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS **17-** ESPIONNAGE À DISTANCE **18-** ÉCOUTE PASSIVE **19-** VOL DE SUPPORTS OU DE DOCUMENTS **20-** VOL DE MATÉRIELS **21-** DIVULGATION INTERNE **22-** DIVULGATION EXTERNE **29-** INFORMATIONS SANS GARANTIE DE L'ORIGINE **30-** PIÉGEAGE DU MATÉRIEL **31-** UTILISATION ILLICITE DU MATÉRIEL **33-** PIÉGEAGE DU LOGICIEL **39-** ABUS DE DROIT **40-** USURPATION DE DROIT **42-** FRAUDE
VI DÉFAILLANCE TECHNIQUE	**23-** PANNE MATÉRIELLE **24-** DYSFONCTIONNEMENT MATÉRIEL **25-** SATURATION DU MATÉRIEL **26-** DYSFONCTIONNEMENT LOGICIEL **28-** ATTEINTE À LA MAINTENABILITÉ DU SI
VII AGRESSION PHYSIQUE	**27-** DESTRUCTION DE MATÉRIELS
VIII ACTIONS ILLICITES	**30-** PIÉGEAGE DU MATÉRIEL **33-** PIÉGEAGE DU LOGICIEL **39-** ABUS DE DROIT **40-** USURPATION DE DROIT **41-** RENIEMENT D'ACTIONS **42-** FRAUDE
IX COMPROMISSION DES FONCTIONS	**20-** VOL DE MATÉRIEL **25-** SATURATION **28-** ATTEINTE À LA MAINTENABILITÉ DU SI **30-** PIÉGEAGE DU MATÉRIEL **31-** UTILISATION ILLICITE DU MATÉRIEL **32-** ALTÉRATION DU LOGICIEL **33-** PIÉGEAGE DU LOGICIEL **34-** COPIE FRAUDULEUSE DE LOGICIEL **35-** UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS **36-** ALTÉRATION DES DONNÉES **39-** ABUS DE DROIT **40-** USURPATION DE DROIT **41-** RENIEMENT D'ACTIONS **42-** FRAUDE **43-** ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL
X ERREUR	**37-** ERREUR DE SAISIE **38-** ERREUR D'UTILISATION

ANNEXE 7 - Menaces génériques (s/systèmes local et distants)

Tableau A7.1	**Fiche de sélection des menaces génériques pour E_L_SITE (site 'local')**											
Menaces génériques	*F*	*V*	*L*	*A*	*S*	*T*	*D*	*C*	*W*	*I*	*E*	*Commentaire*
1- INCENDIE	Menace non retenue (5.2.3.4.b)											
2- DÉGÂT DES EAUX	Menace non retenue (manque de pertinence)											
3- POLLUTION	Menace non retenue (manque de pertinence)											
4- ACCIDENTS MAJEURS	Menace non retenue (manque de pertinence)											
5- PHENOMENE CLIMATIQUE	Menace non retenue (manque de pertinence)											
6- PHENOMENE SISMIQUE	Menace non retenue (manque de pertinence)											
7- PHENOMENE VOLCANIQUE	Menace non retenue (manque de pertinence)											
8- PHENOMENE METEOROLOGIQUE	Menace non retenue (manque de pertinence)											
9- CRUE	Menace non retenue (manque de pertinence)											
10- DEFAILLANCE DE LA CLIMATISATION	Menace non retenue (manque de pertinence)											
11- PERTE D'ALIMENTATION ÉNERGÉTIQUE	Menace non retenue (manque de pertinence)											
12- PERTE DES TÉLÉCOMMUNICATIONS	X	X	X				2					Voir [61].
13- RAYONNEMENTS ELECTROMAGNETIQUES	Menace non retenue (manque de pertinence)											
14- RAYONNEMENTS THERMIQUES	Menace non retenue (manque de pertinence)											
15- IMPULSIONS ELECTROMAGNETIQUES	Menace non retenue (manque de pertinence)											
16- INTERCEPTION DE SIGNAUX PARASITES	Menace non retenue (manque de pertinence)											
17- ESPIONNAGE A DISTANCE	Menace non retenue (manque de pertinence)											
18- ÉCOUTE PASSIVE		X		X				2				Voir [62].
19- VOL DE SUPPORTS OU DE DOCUMENTS	Menace non retenue (manque de pertinence)											
20- VOL DE MATÉRIELS		X		X			3					Voir [63].
21- DIVULGATION INTERNE	Menace non retenue (5.2.3.4.a).											
22- DIVULGATION EXTERNE	Menace non retenue (5.2.3.4.a).											
23- PANNE MATÉRIELLE	X						2					Voir [64].
24- DYSFONCTIONNEMENT MATÉRIEL	X						2					Difficile à apprécier.
25- SATURATION DU MATÉRIEL	Menace non retenue [65].											
26- DYSFONCTIONNEMENT LOGICIEL	X						2	1	1	1		Difficile à apprécier.
27- DESTRUCTION DE MATÉRIELS	Menace non retenue (le matériel n'est pas fragile de nature)											
28- ATTEINTE A LA MAINTENABILITE DU SI	Menace non retenue											
29- INFORMATIONS SANS GARANTIE DE L'ORIGINE	Menace non retenue (5.2.3.4.a).											
30- PIEGEAGE DU MATERIEL	Menace non retenue (5.2.3.4.a).											

[61] Perte partielle de durée limitée en disponibilité.
[62] A priori, la perte en confidentialité impliquerait I_COMM et I_PROFIL (5.2.4.2.f) pour beaucoup d'utilisateurs.
[63] Perte de longue durée en disponibilité pouvant impliquer de nombreux utilisateurs.
[64] Perte de longue durée en disponibilité pouvant impliquer de nombreux utilisateurs.
[65] Les seuls éléments réellement susceptibles d'être saturés sont communs avec E_S_SITE (tableau 8.3, volume 1) et ont donc déjà été envisagés à un niveau d'impact supérieur.

ANNEXE 7 - Menaces génériques (s/systèmes local et distants) (suite)

Tableau A7.1	**Fiche de sélection des menaces génériques pour E_L_SITE (site 'local') (suite)**											
Menaces génériques	*F*	*V*	*L*	*A*	*S*	*T*	*D*	*C*	*W*	*I*	*E*	*Commentaire*
31- UTILISATION ILLICITE DU MATÉRIEL		X	X	X			2	1	2			Voir [66].
32- ALTÉRATION DU LOGICIEL		X	X	X			2			4		Bombe, virus, vers, ...
33- PIÉGEAGE DU LOGICIEL		X	X	X			2	4	3	4	3	Voir [67].
34- COPIE FRAUDULEUSE DE LOGICIEL	Menace non retenue (5.2.3.4.a).											
35- UTILISATION DE LOGICIELS FRAUDULEUX	Menace non retenue (5.2.3.4.a).											
36- ALTÉRATION DES DONNÉES		X	X	X			1	2	2	4		Voir [68].
37- ERREUR D'ENCODAGE	Menace non retenue (manque de pertinence).											
38- ERREUR D'UTILISATION	X						1	2	3			Voir [69].
39- ABUS DE DROIT	Menace non retenue.											
40- USURPATION DE DROIT		X		X			1	2	3	1		Voir [70].

Tableau A7.2	**Fiche de sélection des menaces génériques pour E_D_SITE (sites 'distants')**											
Menaces génériques	*F*	*V*	*L*	*A*	*S*	*T*	*D*	*C*	*W*	*I*	*E*	*Commentaire*
1- INCENDIE	Menace non retenue (8.2.2.d)											
2- DÉGÂT DES EAUX	Menace non retenue (manque probable de pertinence)											
3- POLLUTION	Menace non retenue (manque probable de pertinence)											
4- ACCIDENTS MAJEURS	Menace non retenue (manque probable de pertinence)											
5- PHENOMENE CLIMATIQUE	Menace non retenue (manque probable de pertinence)											
6- PHENOMENE SISMIQUE	Menace non retenue (manque probable de pertinence)											
7- PHENOMENE VOLCANIQUE	Menace non retenue (manque probable de pertinence)											
8- PHENOMENE METEOROLOGIQUE	Menace non retenue (manque probable de pertinence)											
9- CRUE	Menace non retenue (manque probable de pertinence)											
10- DEFAILLANCE DE LA CLIMATISATION	Menace non retenue (manque probable de pertinence)											
11- PERTE D'ALIMENTATION ÉNERGÉTIQUE	Menace non retenue (8.2.2.d)											
12- PERTE DES TÉLÉCOMMUNICATIONS	X	X	X				1					Voir [71].
13- RAYONNEMENTS ELECTROMAGNETIQUES	Menace non retenue (manque probable de pertinence)											
14- RAYONNEMENTS THERMIQUES	Menace non retenue (manque probable de pertinence)											
15- IMPULSIONS ELECTROMAGNETIQUES	Menace non retenue (manque probable de pertinence)											
16- INTERCEPTION DE SIGNAUX PARASITES	Menace non retenue (manque probable de pertinence)											

[66] Permettrait la consultation des catégories d'informations I_PROFIL et I_COMM;
[67] Cheval de Troie, trappe, canal caché: impact important du fait de la présence dans E_L_SITE du poste de développement.
[68] Données transitant par le LAN: I_COMM et I_PROFIL.
[69] Atteinte en disponibilité pour cause de DoS involontaire; atteinte en confidentialité et en imputabilité pour cause de non déconnexion (4.5.1.i).
[70] Imputabilité: rejeu (4.5.1.h) ou IP HI-jacking (4.5.1.j).
[71] Perte de durée limitée en disponibilité pour un ou deux utilisateurs seulement.

ANNEXE 7 - Menaces génériques (s/systèmes local et distants) (suite)

Tableau A7.2	**Fiche de sélection des menaces génériques pour E_D_SITE (sites 'distants') (suite)**											
Menaces génériques	*F*	*V*	*L*	*A*	*S*	*T*	*D*	*C*	*W*	*I*	*E*	*Commentaire*
17- ESPIONNAGE A DISTANCE	Menace non retenue (manque probable de pertinence)											
18- ÉCOUTE PASSIVE		X		X				1				Voir [72].
20- VOL DE MATÉRIELS		X		X			1					Voir [73].
21- DIVULGATION INTERNE	X	X		X				2	4			Voir [74].
22- DIVULGATION EXTERNE	X	X		X				2	4			Voir [75].
23- PANNE MATÉRIELLE	X						1					Voir [76].
24- DYSFONCTIONNEMENT MATÉRIEL	X						1					Voir [77].
25- SATURATION DU MATÉRIEL	X	X	X				1					Voir [78] [79].
26- DYSFONCTIONNEMENT LOGICIEL	X						1	1	1	1		Difficile à apprécier.
27- DESTRUCTION DE MATÉRIELS	Menace non retenue (le matériel n'est probablement pas fragile de nature)											
28- ATTEINTE A LA MAINTENABILITE DU SI	Menace non retenue											
29- INFORMATIONS SANS GARANTIE DE L'ORIGINE	Menace non retenue.											
30- PIEGEAGE DU MATERIEL	Menace non retenue.											
31- UTILISATION ILLICITE DU MATÉRIEL		X	X	X			1	1	1			Voir [80].
32- ALTÉRATION DU LOGICIEL		X	X	X			1			4		Bombe, virus, vers, ...
33- PIÉGEAGE DU LOGICIEL		X	X	X			1	1		4		Voir [81].
34- COPIE FRAUDULEUSE DE LOGICIEL	Menace non retenue.											
35- UTILISATION DE LOGICIELS FRAUDULEUX	Menace non retenue (hypothèse).											
36- ALTÉRATION DES DONNÉES		X	X	X			1		1	4		Voir [82].
37- ERREUR D'ENCODAGE	Menace non retenue (manque de pertinence).											
38- ERREUR D'UTILISATION	X						1	1	2			Voir [83].
39- ABUS DE DROIT	Menace non retenue.											
40- USURPATION DE DROIT		X		X			1	2	3			Voir [84].

[72] A priori, la perte en confidentialité impliquerait I_COMM et I_PROFIL pour beaucoup d'utilisateurs.
[73] Perte de longue durée en disponibilité pour un ou deux utilisateurs seulement.
[74] Le seul élément du SC qu'un client pourrait divulguer est son propre secret.
[75] Le seul élément du SC qu'un client pourrait divulguer est son propre secret.
[76] Perte de longue durée en disponibilité pour un ou deux utilisateurs seulement.
[77] Perte de longue durée en disponibilité pour un ou deux utilisateurs seulement.
[78] Engorgement (atteinte accidentelle mais structurelle) ou parasitage intense et continu (atteinte volontaire).
[79] Perte Perte de longue durée en disponibilité pour un ou deux utilisateurs seulement.
[80] Permettrait la consultation et l'altération des catégories d'informations I_PROFIL et I_COMM;
[81] Cheval de Troie, trappe, canal caché.
[82] Données transitant par le LAN: I_COMM et I_PROFIL.
[83] Atteinte en disponibilité pour cause de DoS involontaire; atteinte en confidentialité et en imputabilité pour cause de non déconnexion (4.5.1.i).
[84] Imputabilité: rejeu (4.5.1.h) ou IP HI-jacking (4.5.1.j).

ANNEXE 8 - Répertoire des vulnérabilités spécifiques (EBIOS)

Tableau A8.1	**Vulnérabilités spécifiques pour l'entité MATERIEL & LOGICIEL *(ML)***
Menace	*Vulnérabilités associées*
13	- Matériel sensible aux rayonnements électromagnétiques
14	- Matériel sensible aux rayonnements thermiques
15	- Matériel sensible à l'IEM
16	- Matériel susceptible d'émettre des rayonnements parasites compromettants
20	*20ML1*- Matériels attractifs (valeurs marchande, technologique, stratégique) *20ML2*- Matériels mobiles ou aisément transportable (portables,...)
21	- Systèmes permettant un échange facile de l'information (disquette, messagerie, télécopieur, téléphone,...)
22	- Systèmes permettant un échange facile de l'information (disquette, messagerie, télécopieur, téléphone,...)
23	*23ML1* - Fiabilité des ressources - Défaut de maintenance - Mauvaises conditions d'utilisation
24	- Possibilité de mal configurer, installer ou modifier les ressources *24ML2*- Usure des matériels - Ressources insuffisamment recettées - Possibilité d'incompatibilité entre différentes ressources
25	*25ML1*- Possibilité que les ressources soient soumises à un nombre trop important de requêtes - Ressources mal dimensionnées
26	*26ML1*- Mauvaise conception, mauvaise installation des logiciels *26ML2*- Mauvaise gestion des versions et configurations logicielles
27	- Fragilité des matériels (ex. : systèmes embarqués)
28	- Matériels/logiciels spécifiques - Matériels obsolètes - Matériels à configurations non évolutives
30	- Possibilité de pose d'éléments matériels additionnels pour stocker, transmettre ou altérer
31	*31ML1*- Le système est connecté à des réseaux externes - Le système est, par nature, accessible et utilisable par tous (minitel...). *31ML3*- Le matériel utilisé permet un autre usage que celui qui est prévu (développement de logiciels non destinés à 'organisme...) *31ML4*- Possibilité d'utiliser une porte dérobée (trappe) dans un programme *31ML5- Facilité de pénétrer le système*
32	*32ML1*- Possibilité de modifier ou changer les applicatifs *32ML2*- Possibilité d'effacer ou modifier des fichiers-programmes *32ML3*- Possibilité d'être infecté par un virus *32ML4*- Possibilité d'exploiter le fonctionnement asynchrone de certaines parties ou commandes du système d'exploitation *32ML5- Facilité de pénétrer le système*
33	*33ML1*- Possibilité de créer ou modifier des commandes systèmes *33ML2*- Possibilité d'implanter des programmes pirates *33ML3*- Possibilité de modifier ou changer les applicatifs *33ML4*- Possibilité d'existence de fonctions cachées introduites en phase de conception et développement - Utilisation de matériel non évalués *33ML6*- Possibilité d'effacer ou modifier des fichiers-programmes *32ML7- Facilité de pénétrer le système*
34	- Possibilité de copier facilement des logiciels ou progiciels - Logiciels attractifs ou "grand public"
35	- Possibilité que les système fonctionnent avec des logiciels copiés illicitement ou contrefaits
36	*36ML1*- Le système permet, par nature, d'accéder à des données ***locales*** *36ML2*- ***Possibilité d'agir sur les données transmises*** *36ML3- Facilité de pénétrer le système*
37	*37ML1- Matériel d'utilisation complexe ou peu ergonomique*
38	*38ML1*- Matériel d'utilisation complexe ou peu ergonomique
40	*40ML1*- Le système est connecté à des réseaux externes *40ML2*- Facilité de pénétrer le ssystème
41	- Le système est, par nature, accessible et utilisable par tous (minitel...). - Le traitement nécessite une intervention humaine
42	- Le détournement des fonctions réalisées, par le système, permet l'obtention d'un avantage (promotion, gain...) ou cause un préjudice à des tiers
43	- Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran...)

Note: Les ajoûts ou modifications que nous avons introduits sont en caractères *italiques*.

ANNEXE 8 - Répertoire des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A8.2	**Vulnérabilités spécifiques pour l'entité RESEAUX INTERNES *(RI)***
Menace	*Vulnérabilités associées*
13	- Matériel sensible aux rayonnements électromagnétiques
14	- Matériel sensible aux rayonnements thermiques
15	- Matériel sensible à l'IEM
16	- Matériel susceptible d'émettre des rayonnements parasites compromettants
18	*18RI1*- Matériel ayant des éléments permettant l'écoute passive (câblage, prises de connexion...)
20	*20RI1*- Matériels attractifs (valeur marchande, technologique, stratégique) *20RI1*- Matériels de faible encombrement
21	- Systèmes permettant un échange aisé de l'information (téléphone, télécopieur, messagerie)
22	- Systèmes permettant un échange facile de l'information (téléphone, télécopieur, messagerie)
23	*23RI1*- Fiabilité des ressources - Défaut de maintenance - Mauvaises conditions d'utilisation
24	- Possibilité de mal configurer, installer ou modifier les ressources *24RI2*- Usure des matériels - Ressources insuffisamment recettées - Possibilité d'incompatibilité entre différentes ressources
25	*25RI1*- Possibilité que les ressources soient soumises à un nombre trop important de requêtes - Ressources mal dimensionnées
26	*26RI1*- Mauvaise conception, mauvaise installation des logiciels *26RI2*- Mauvaise gestion des versions et configurations logicielles
27	- Fragilité des matériels (ex. : systèmes embarqués)
28	- Utilisation de réseaux limités dans les capacités et les infrastructures
30	- Possibilité de pose d'éléments matériels additionnels pour stocker, transmettre ou altérer
31	*31RI1*- Le système est connecté à des réseaux externes - Le système est, par nature, accessible et utilisable par tous (minitel...). *31RI3*- Le matériel utilisé permet un autre usage que celui qui est prévu .
32	- Possibilité de modifier ou changer les applicatifs - Possibilité d'effacer ou modifier des fichiers-programmes - Possibilité d'altération par un ver
33	- Possibilité de créer ou modifier des commandes systèmes - Possibilité d'implanter des programmes pirates - Possibilité de modifier ou changer les applicatifs - Possibilité d'existence de fonctions cachées introduites en phase de conception ou développement - Possibilité d'effacer ou modifier des fichiers-programmes
34	- Possibilité de copier facilement des logiciels ou progiciels - Logiciels attractifs ou "grand public"
35	- Possibilité que les système fonctionnent avec des logiciels copiés illicitement ou contrefaits
36	*36RI1*- Possibilité d'agir sur les données transmises par l'intermédiaire du média de communication.
38	- Matériel d'utilisation complexe ou peu ergonomique
40	- Le système est connecté à des réseaux externes
41	- Le système est, par nature, accessible et utilisable par tous (minitel...). - Le traitement nécessite une intervention humaine
42	- Le détournement des fonctions réalisées, par le système, permet l'obtention d'un avantage (promotion, gain...) ou cause un préjudice à des tiers
43	- Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (transmission par voie hertzienne...)

Note: Les ajoûts ou modifications que nous avons introduits sont en caractères *italiques*.

ANNEXE 8 - Répertoire des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A8.3	**Vulnérabilités spécifiques pour l'entité RESEAUX EXTERNES *(RE)***
Menace	*Vulnérabilités associées*
12	*12RE1*- Le réseau peut être sujet à des défaillances graves *12RE2*- Le réseau peut être détruit
15	- Le réseau peut être affecté par une IEM
18	*18RE1*- Le réseau a des caractéristiques techniques qui permettent l'écoute passive
21	- Le réseau facilite, par nature, la divulgation à l'intérieur de l'organisme d'informations (téléphone, fax, messagerie...)
22	- Le réseau facilite, par nature, la divulgation à l'extérieur d'informations (téléphone, fax, messagerie...)
25	- Le réseau peut induire des surcharges pour le système *25RE2*- Le réseau permet de soumettre le système à des surchages de requêtes ou un parasitage intense *25RE3- Possibilité que les ressources soient soumises à un nombre trop important de requêtes*
26	- Les caractéristiques du réseau créent des disfonctionnements aux logiciels du système (problèmes de compatibilités entre protocoles...)
28	- La maintenance ou l'exploitation du système se fait par l'intermédiaire du réseau
31	*31RE1*- Le réseau permet d'utiliser les ressources du système depuis l'extérieur
32	*32RE1*- Le réseau permet de modifier ou d'agir sur les logiciels des ressources du système *32RE2*- Le réseau permet d'introduire des logiciels à effets malicieux tels que vers, virus, bombes logiques...
33	- Le réseau permet de modifier ou d'agir sur les logiciels des ressources du système
34	- Le réseau permet le téléchargement de logiciels
35	- Le réseau permet le téléchargement de logiciels
36	*36RE1*- Possibilité d'agir sur les données transmises par l'intermédiaire du média de communication.
40	*40RE1*- Le réseau donne la possibilité à des personnes non habilitées de tenter de bénéficier de droits qu'ils n'ont pas
41	- Le réseau permet d'utiliser les services du système depuis l'extérieur, sans identification / authentification (minitel, fax, téléphone...)

Note: Les ajoûts ou modifications que nous avons introduits sont en caractères *italiques*.

ANNEXE 8 - Répertoire des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A8.4	Vulnérabilités spécifiques pour l'entité SITE *(S)*
Menace	*Vulnérabilités associées*
1	- Manque de cohérence des mesures contre l'incendie - Manque de cohérence des mesures incendie avec le système informatique
2	- Canalisations d'eau à proximité du système informatique
3	- Proximité d'une source de pollution (fumées, vapeurs,...) - Le système est situé dans une atmosphère polluée (hangar, atelier,...)
4	- Proximité de points dangereux (explosions, implosions) - Possibilité de destruction causée par des collisions, des chutes (chute d'aéronefs, accidents ferroviaires,...)
5	- Absence de protection du site contre les rigueurs climatiques
6	- Bâtiments hors normes anti-sismiques
7	- Proximité d'un volcan actif
8	- Absence de protection contre la foudre - Absence de protection contre les phénomènes météorologiques (tempête, ouragan, cyclône,...)
9	- Absence de protection contre la montée des eaux
10	- Mauvaise fiabilité du matériel de climatisation - Facilité d'accès à la centrale de climatisation
11	- Pas de dispositifs de protection contre les coupures du réseau EDF - Faiblesses des caractéristiques de la centrale électrique interne - Faiblesses des caractéristiques du réseau secouru
12	- Facilité d'accès au commutateur interne - Défauts d'exploitation du réseau téléphonique interne - Dysfonctionnement des réseaux externes (France Télécom,...)
13	- Proximité d'une source de rayonnements électro-magnétiques
14	- Proximité d'une source de rayonnements thermiques
15	- Possibilité pour le système d'être soumis à des IEM
16	- Situation facilitant la capture des signaux parasites compromettants - Facilité de branchement sur des équipements conducteurs de courant (câbles électriques, tuyauteries,...)
17	- Facilité d'observations par moyens optiques - Facilité de surveillance de l'activité
18	*18S1*- Facilité de pénétrer sur le site - Faciliter de capter les transmissions à l'extérieur du site *18S3- Facilité de pénétrer les locaux*
19	*19S1*- Facilité de pénétrer sur le site *19S2*- Facilité de pénétrer dans les locaux
20	- Facilité de pénétrer sur le site *20S2*- Facilité de pénétrer dans les locaux - Facilité de franchir le contrôle d'accès - Facilité de pénétrer par des accès indirects
30	- Facilité de pénétrer dans le site - Facilité de pénétrer dans les locaux - Facilité de franchir le contrôle d'accès - Facilité de pénétrer par des accès indirects
31	- Facilité de pénétrer dans le site *31S2*- Facilité de pénétrer dans les locaux - Facilité de franchir le contrôle d'accès - Facilité de pénétrer par des accès indirects
32	*32S1- Facilité de pénétrer dans les locaux*
33	- Facilité de pénétrer dans le site *33S2*- Facilité de pénétrer dans les locaux - Facilité de franchir le contrôle d'accès - Facilité de pénétrer par des accès indirects
34	- Facilité de pénétrer dans le site *33S3*- Facilité de pénétrer dans les locaux - Facilité de franchir le contrôle d'accès - Facilité de pénétrer par des accès indirects
36	- Facilité de pénétrer dans le site *36S2*- Facilité de pénétrer dans les locaux - Facilité de franchir le contrôle d'accès - Facilité de pénétrer par des accès indirects
40	*40S1- Facilité de pénétrer dans les locaux*

Note: Les ajoûts ou modifications que nous avons introduits sont en caractères *italiques*.

ANNEXE 8 - Répertoire des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A8.5	**Vulnérabilités spécifiques pour l'entité PERSONNEL *(P)* (suite)**
Menace	*Vulnérabilités associées*
19	*19P1-* Manque de vigilance - Absence de règles morales ou d'éthique - Peu de sensibilisation aux problèmes de sécurité
20	- Absence de règles morales ou d'éthique
21	- Non respect du devoir de réserve - Peu de sensibilisation aux problèmes de sécurité
22	- Non respect du devoir de réserve - Obtention d'un avantage - Personnel manipulable - Peu de sensibilisation aux problèmes de sécurité
27	- Personnel peu soigneux
28	- Méconnaisance des enjeux du système pour l'organisme - Méconnaissance des protections en matière d'assurance, - Méconnaissance du droit - Négligence, imprévision
29	- Absence de rigueur - Peu de sensibilisation aux problèmes de sécurité - Crédulité
30	- Obtention d'un avantage - Personnel manipulable
31	- Absence de règles morales ou d'éthique - Droits accordés en dehors du besoin légitime - Obtention d'un avantage
32	- Peu de sensibilisation aux problèmes de sécurité - Situation conflictuelle entre personnes - Personnel manipulable
33	- Absence de règles morales ou d'éthique - Obtention d'un avantage - Situation conflictuelle entre personnes - Personnel manipulable
34	- Absence de règles morales ou d'éthique - Non respect des règlements - Obtention d'un avantage - Personnel manipulable
35	- Non respect des règlements - Méconnaisance des lois
36	- Obtention d'un avantage - Situation conflictuelle entre personnes - Personnel manipulable
37	- Personnel peu habitué à la saisie *37P2-* Conditions de travail défavorables - Absence de motivation pour les travaux associés à la saisie
38	- Personnel utilisateur peu ou mal formé - Manque de professionnalisme - Non respect des consignes
39	- Prééminence de la catégorie de personnel - Absence de règles morales ou d'éthique - La notion de droit n'est pas définie pour le personnel
40	- Absence de règles morales ou d'éthique - Situation conflictuelle entre personnes - Obtention d'un avantage - Droits accordés en dehors du besoin légitime
41	- Problèmes de responsabilité - Manque de confiance dans l'organisation - Situation conflictuelle entre personnes
42	- Absence de règles morales ou d'éthique - Obtention d'un avantage - Non respect des règlements

Note: Les ajoûts ou modifications que nous avons introduits sont en caractères *italiques*.

ANNEXE 8 - Répertoire des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A8.5	**Vulnérabilités spécifiques pour l'entité PERSONNEL *(P)* (suite)**
Menace	*Vulnérabilités associées*
43	- Indisponibilité causée par l'absentéisme - Indisponibilité causée par la maladie - Indisponibilité provoquée (agression physique, prise d'otage...) - Problèmes sociaux

Tableau A8.6	**Vulnérabilités spécifiques pour l'entité ORGANISATION *(O)***
Menace	*Vulnérabilités associées*
1	- Absence de consignes (alerte, prévention, formation...) - Absence d'organisation sécurité incendie
2	- Absence de consignes (alerte, prévention, formation...)
3	- Absence de consignes (alerte, prévention, formation...)
4	- Absence de consignes (alerte, prévention,...) - Absence d'information
5	- Absence de consignes (alerte, prévention,...) - Absence d'information
6	- Absence de consignes (alerte, prévention,...) - Absence d'information
7	- Absence de consignes (alerte, prévention,...) - Absence d'information
8	- Absence de consignes (alerte, prévention,...) - Absence d'information
9	- Absence de consignes (alerte, prévention,...) - Absence d'information
17	- Absence d'organisation de sécurité - Absence de sensibilisation aux problèmes de sécurité
18	- Absence de sensibilisation aux problèmes de confidentialité
19	- Absence de sensibilisation aux problèmes de sécurité
20	- Absence de sensibilisation aux problèmes de sécurité - Absence de prise en compte du matériel par les utilisateurs
21	- Absence de procédures de contrôle de l'utilisation des outils de communication - Absence de sensibilisation aux problèmes de confidentialité
22	- Absence de procédures de contrôle d l'utilisation des outils de communication - Absence de sensibilisation aux problèmes de sécurité - Absence de la notion de "devoir de réserve"
23	- Absence d'un service ou d'un responsable de la maintenance - Absence de consignes relatives à l'utilisation du matériel
24	- Absence d'un service ou d'un responsable informatique - Absence de consignes relatives à l'utilisation du matériel informatique
25	- Absence de consignes relatives à l'utilisation du matériel informatique
26	- Absence d'un service ou d'un responsable informatique
28	- Absence de plan de protection contre les défaillances des sociétés de maintenance - Absence de plans de formation à la gestion des systèmes utilisés - Mauvaise organisation du service gérant les marchés, du service gérant les budgets
29	- Absence de consignes de travail - Absence de sensibilisation aux problèmes de sécurité - Absence de protocoles de sélection des informations - Confiance exagérée dans les interlocuteurs ou les serveurs tiers - Absence de garanties dans les prestations fournies
30	- Absence de plan de contrôle des matériels
31	- Possibilité d'utiliser les ressources sans contrôle (matériel en libre service...) - Absence de consignes relatives à l'utilisation du matériel informatique

Note: Les ajoûts ou modifications que nous avons introduits sont en caractères *italiques*.

ANNEXE 8 - Répertoire des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A8.6	**Vulnérabilités spécifiques pour l'entité ORGANISATION *(O)* (suite)**
Menace	*Vulnérabilités associées*
32	- Absence de consignes relatives à l'utilisation du matériel informatique - Absence de sensibilisation aux problèmes de sécurité informatiques - Absence de procédures de contrôle des disquettes extérieures
33	- Absence de mesures de sécurité dans les phases de conception, installation et exploitation
34	- Absence de sensibilisation ou d'information sur la législation des droits d'auteur
35	- Absence de sensibilisation ou d'information sur la législation des droits d'auteur
36	- Absence d'habilitation du personnel - Absence de consignes relatives à l'utilisation du matériel informatique - Absence de contrôle des opérations effectuées
38	- Absence de formation sur les matériels ou logiciels utilisés.
39	- Absence de définition du droit d'en connaître - Absence d'un règlement définissant les droits - Les attributions des utilisateurs ne sont pas clairement définies
40	- Possibilité d'utiliser les ressources sans contrôle (matériel en libre service...) - Absence d'habilitation du personnel
41	- Possibilité d'utiliser les ressources sans contrôle (matériel en libre service...) - Absence de définition des responsabilités
42	- Absence de procédures de contrôles sur les actions effectuées par le personnel

Note: Les ajoûts ou modifications que nous avons introduits sont en caractères *italiques*.

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS)

Tableau A9.1	**Sous-système *serveur* (E_S_SITE)**									
Menaces et vulnérabilités associées	*E_S_ SVHW*	*E_S_ FWHW*	*E_S_ SVSW*	*E_S_ FWSW*	*LAN*	*WAN[85] (LLine)*	*WAN[86] (INET)*	*E_S_ SITE*	*E_S_ ADMIN*	*Commentaire*
12- Pertes des télécommunications										
12RE1- Le réseau externe peut être soumis à des défaillances graves						0,00	0,50			
12RE2- Le réseau externe peut être détruit						0,25[87]	0,00[88]			
18- Ecoute passive										
18RI1- Matériel ayant des éléments permettant l'écoute passive					0,75					
18RE1- Réseau ayant des caractéristiques permettant l'écoute passive						0,50	0,50			
18S3- Facilité de pénétrer les locaux								0,50		
19- Vol de supports ou de documents										
19S2- Facilité de pénétrer le site								0,50		
19P1- Manque de vigilance									0,25	
20- Vol de matériel										
20ML1- Matériels attractifs (valeur marchande, ...)	0,50	0,50	0,75	0,75						
20RI1- Matériels attractifs (valeur marchande, ...)					0,25					
20ML2- Matériels mobiles ou aisément transportables	0,50	0,50	0,75	0,75						
20RI2- Matériels de faible encombrement					0,75					
20S2- Facilité de pénétrer les locaux								0,50		
23- Panne matérielle										
23ML1- Fiabilité des ressources	0,25	0,25								
23RI1- Fiabilité des ressources					0,25					

[85] LLine: ligne louée.
[86] INET: Internet
[87] Un engin de génie civil pourrait trancher la boucle locale (impact sur la ligne louée comme sur la ligne backup)
[88] Selon un de ses principes fondateurs.

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.1	Sous-système *serveur* (E_S_SITE) (suite)									
Menaces et vulnérabilités associées	*E_S_ SVHW*	*E_S_ FWHW*	*E_S_ SVSW*	*E_S_ FWSW*	*LAN*	*WAN[89] (LLine)*	*WAN[90] (INET)*	*E_S_ SITE*	*E_S_ ADMIN*	*Commentaire*
24- Dysfonctionnement matériel										
24ML1- Usure des matériels	0,25	0,25			0,25					
25- Saturation du matériel										
25ML1- Ressources soumises à un nombre trop important de requêtes[91]	0,25	0,25	0,25[92]	0,25[93]						
25RE2- Le réseau permet les surcharges / le parasitage							0,50			
25RI1- Ressources peuvent être soumises à un nombre trop important de requ.					0,25					
25RE3- Ressources peuvent être soumises à un nombre trop important de requ.						0,50				
26- Dysfonctionnement logiciel										
26ML1- Mauvaise conception ou installation des logiciels			0,25	0,25						
26ML2- Mauvaise gestion des versions et configurations logicielles			0,25	0,25						
31- Utilisation illicite du matériel										
31ML1- Système connecté à des réseaux externes	0,25	0,25	0,25	0,25						
31ML3- Matériel permet un autre usage que celui pour lequel il est prévu	0,00	0,00	0,25	0,25						
31ML4- Possibilité d'utilisation d'une porte dérobée dans un logiciel			0,00	0,00						
31RE1- Le réseau permet d'utiliser les resources du système depuis l'extérieur							0,25			
31S2- Facilité de pénétrer les locaux								0,50		
31ML5- Facilité de pénétrer le système			0,25	0,25						

[89] LLine: ligne louée.
[90] INET: Internet
[91] Matériels et LAN: selon probabilité de dysfonctionnement.
[92] Protégé par sa configuration et par les dispositifs de protection logique
[93] Conçu pour y résister.

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.1	**Sous-système *serveur* (E_S_SITE) (suite)**									
Menaces et vulnérabilités associées	*E_S_ SVHW*	*E_S_ FWHW*	*E_S_ SVSW*	*E_S_ FWSW*	*LAN*	*WAN[94] (LLine)*	*WAN[95] (INET)*	*E_S_ SITE*	*E_S_ ADMIN*	*Commentaire*
32- Altération du logiciel										
32ML1- Possibilité de modifier ou changer les applicatifs			0,25	0,25						
32ML2- Possibilité d'effacer (ou de modifier) des fichiers-programmes			0,50	0,50						
32ML3- Possibilité d'être infecé par un virus ou un vers			0,25	0,25						
32S2- Facilité de pénétrer les locaux								0,50		
32ML5- Facilité de pénétrer le système			0,25	0,25						
32RE2- Le réseau permet d'introduire des logiciels malicieux (virus, vers)							0,50			
33- Piégeage du logiciel										
33ML1- Possibilité de créer (ou modifier) des commandes système			0,25	0,25						
33ML2- Possibilité d'implanter des programmes pirates			0,50	0,50						
33ML3- Possibilité de modifier ou changer les applicatifs			0,25	0,25						
33ML4- Possibilité d'existence de fonctions cachée (concep. ou dével.)			0,00	0,00						
33ML6- Possibilité d'effacer (ou de modifier) des fichiers-programmes			0,50	0,50						
33S2- Facilité de pénétrer les locaux								0,50		
33ML7- Facilité de pénétrer le système			0,25	0,25						
36- Altération des données										
36ML1- Le système permet d'accéder à des données locales	0,00	0,00	0,50	0,50						
36ML2- Possibilité d'agir sur les données transmises	0,00	0,00	0,25	0,25						
36RI1- Possibilité d'agir sur les données transmises					0,25					
36RE1- Possibilité d'agir sur les données transmises						0,25	0,25			
36S2- Facilité de pénétrer les locaux								0,50		
36ML3- Facilité de pénétrer le système			0,25	0,25						

[94] LLine: ligne louée.
[95] INET: Internet

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.1	**Sous-système *serveur* (E_S_SITE) (suite)**									
Menaces et vulnérabilités associées	*E_S_ SVHW*	*E_S_ FWHW*	*E_S_ SVSW*	*E_S_ FWSW*	*LAN*	*WAN[96] (LLine)*	*WAN[97] (INET)*	*E_S_ SITE*	*E_S_ ADMIN*	*Commentaire*
37 Erreur de saisie										
37ML1- Matériel d'utilisation complexe ou peu ergonomique			0,25	0,25						
37P2- Conditions de travail défavorables									0,25	
40- Usurpation de droits										
40ML1- Le système est connecté à des réseaux externes			0,25	0,25						
40S2- Facilité de pénétrer les locaux								0,50		
40ML2- Facilité de pénétrer le système			0,25	0,25						

Tableau A9.2	**Sous-système *local* (E_L_SITE)**										
Menaces et vulnérabilités associées	*E_L DWHW*	*E_L CWHW*	*E_L DWSW*	*E_L CWSW*	*LAN*	*WAN (L.Line)*	*WAN (INET)*	*E_L_ SITE*	*E_L_ DEV*	*E_L_ USR*	*Commentaire*
12- Pertes des télécommunications[98]											
12RE1- Le réseau externe peut être soumis à des défaillances graves						0,00	0,50				
12RE2- Le réseau externe peut être détruit						0,25	0,00				
18- Ecoute passive											
18RI1- Matériel ayant des éléments permettant l'écoute passive					0,75						
18RE1- Réseau ayant des caractéristiques permettant l'écoute passive						0,50	0,50				
18S3- Facilité de pénétrer les locaux								0,75			

[96] LLine: ligne louée.
[97] INET: Internet
[98] Identique à E_S_SITE (entités communes).

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.2	**Sous-système *local* (E_L_SITE) (suite)**										
Menaces et vulnérabilités associées	*E_L DWHW*	*E_L CWHW*	*E_L DWSW*	*E_L CWSW*	*LAN*	*WAN (L.Line)*	*WAN (INET)*	*E_L_ SITE*	*E_L_ DEV*	*E_L_ USR*	*Commentaire*
20- Vol de matériel											
20ML1- Matériels attractifs (valeur marchande, ...)	0,50	0,50	0,75	0,75							
20RI11- Matériels attractifs (valeur marchande, ...)					0,25						
20ML2- Matériels mobiles ou aisément transportables	0,50	0,50	0,75	0,75							
20RI2- Matériels de faible encombrement					0,75						
20S2- Facilité de pénétrer les locaux								0,75			
23- Panne matérielle											
23ML1- Fiabilité des ressources	0,25	0,25			0,25						
24- Dysfonctionnement matériel											
24ML1- Usure des matériels	0,25	0,25			0,25						
25- Saturation du matériel											
25ML1- Ressources soumises à un nombre trop important de requêtes	0,00	0,00	0,00	0,00							
25RI1- Ressources soumises à un nombre trop important de requêtes					0,25						
25RE3- Ressources soumises à un nombre trop important de requêtes						0,50					
25RE2- Le réseau permet les surcharges / le parasitage							0,50				
26- Dysfonctionnement logiciel											
26ML1- Mauvaise conception ou installation des logiciels			0,25	0,25							
26ML2- Mauvaise gestion des versions et configurations logicielles			0,25	0,25							

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.2 | **Sous-système *local* (E_L_SITE) (suite)**

Menaces et vulnérabilités associées	*E_L DWHW*	*E_L CWHW*	*E_L DWSW*	*E_L CWSW*	*LAN*	*WAN (L.Line)*	*WAN (INET)*	*E_L_ SITE*	*E_L_ DEV*	*E_L_ USR*	*Commentaire*
31- Utilisation illicite du matériel											
31ML1- Système connecté à des réseaux externes	0,75	0,75	0,75	0,75	0,75						
31ML4- Possibilité d'utilisation d'une porte dérobée dans un logiciel			0,25	0,25							
31RE1- Le réseau permet d'utiliser les resSources du système depuis l'extérieur							0,25				
31S2- Facilité de pénétrer les locaux								0,75			
31ML5- facilité de pénétrer le système			0,50	0,50							
32- Altération du logiciel											
32ML1- Possibilité de modifier ou changer les applicatifs			0,50	0,50							
32ML2- Possibilité d'effacer (ou de modifier) des fichiers-programmes			0,75	0,75							
32ML3- Possibilité d'être infecté par un virus			0,50	0,50							
32S2- facilité de pénétrer les locaux								0,75			
32ML5- facilité de pénétrer le système			0,50	0,50							
32RE2- Le réseau permet d'introduire des logiciels malicieux (vers, virus)							0,50				
33- Piégeage du logiciel											
33ML1- Possibilité de créer (ou modifier) des commandes système			0,50	0,50							
33ML2- Possibilité d'implanter des programmes pirates			0,75	0,75							
33ML3- Possibilité de modifier ou changer les applicatifs			0,50	0,50							
33ML4- Possibilité d'existence de fonctions cachée (concep. ou dével.)			0,25	0,25							
33ML6- Possibilité d'effacer(ou de modifier) des fichiers-programmes			0,75	0,75							
33S2- facilité de pénétrer les locaux								0,75			
33ML7- facilité de pénétrer le système			0,50	0,50							

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.2 | **Sous-système *local* (E_L_SITE) (suite)**

Menaces et vulnérabilités associées	*E_L_DWHW*	*E_L_CWHW*	*E_L_DWSW*	*E_L_CWSW*	*LAN*	*WAN (L.Line)*	*WAN (INET)*	*E_L_SITE*	*E_L_DEV*	*E_L_USR*	*Commentaire*
36- Altération des données											
36ML1- Le système permet d'accéder à des données locales	0,00	0,00	0,00	0,00							
36ML2- Possibilité d'agir sur les données transmises	0,25	0,50	0,25	0,50							
36RI1- Possibilité d'agir sur les données transmises					0,25						
36RE1- Possibilité d'agir sur les données transmises[99]						0,25	0,25				
36S2- facilité de pénétrer les locaux								0,75			
36ML3- Facilité de pénétrer le système			0,50	0,50							
38- Erreur d'utilisation											
38P1- Personnel utilisateur peu ou mal formé										0,50	
40- Usurpation de droits											
40ML1- Le système est connecté à des réseaux externes			0,25	0,25							
40ML2- Facilité de pénétrer le système			0,50	0,50							
40S2- Facilité de pénétrer les locaux								0,75			

Tableau A9.3 | **Sous-système *distant* (E_D_SITE)**

Menaces et vulnérabilités associées	*E_D_CWHW*	*E_D_CWSW*	*LAN*	*WAN (dialup)*	*WAN (INET)*	*E_D_SITE*	*E_D_USR*	*Commentai-re*
12- Pertes des télécommunications								
12RE1- Le réseau externe peut être soumis à des défaillances graves				0,25	0,50			
12RE2- Le réseau externe peut être détruit				0,25	0,00			
18- Ecoute passive								
18RI1- Matériel ayant des éléments permettant l'écoute passive			0,75					
18RE1- Réseau ayant des caractéristiques permettant l'écoute passive				0,50	0,50			
18S3- Facilité de pénétrer les locaux						1,00		

[99] Identique à E_S_SITE (entités communes).

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.3	**Sous-système *distant* (E_D_SITE) (suite)**							
Menaces et vulnérabilités associées	*E_D_ CWHW*	*E_D_ CWSW*	*LAN*	*WAN (dialup)*	*WAN (INET)*	*E_D_ SITE*	*E_D_ USR*	*Commentai-re*
20- Vol de matériel								
20ML1- Matériels attractifs (valeur marchande, ...)	0,50	0,75						
20RI11- Matériels attractifs (valeur marchande, ...)			0,25					
20ML2- Matériels mobiles ou aisément transportables	0,50	0,75						
20RI2- Matériels de faible encombrement			0,75					
20S2- Facilité de pénétrer les locaux						1,00		
23- Panne matérielle								
23ML1- Fiabilité des ressources	0,25		0,25					
24- Dysfonctionnement matériel								
24ML1- Usure des matériels	0,25		0,25					
25- Saturation du matériel								
25ML1- Ressources soumises à un nombre trop important de requêtes	0,50	0,50						
25RI1- Ressources soumises à un nombre trop important de requêtes			0,50					
25RE3- Ressources soumises à un nombre trop important de requêtes				0,75				
25RE2- Le réseau permet les surcharges / le parasitage					0,50			
26- Dysfonctionnement logiciel								
26ML1- Mauvaise conception ou installation des logiciels		0,25						
26ML2- Mauvaise gestion des versions et configurations logicielles		0,25						
31- Utilisation illicite du matériel								
31ML1- Système connecté à des réseaux externes	0,75	0,75	0,75					
31ML3- Matériel permet un autre usage que celui pour lequel il est prévu	0,75	0,75	0,75					
31ML4- Possibilité d'utilisation d'une porte dérobée dans un logiciel		0,25						
31RE1- Le réseau permet d'utiliser les resources du système depuis l'extérieur					0,25			
31S2- Facilité de pénétrer les locaux						1,00		

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.3	**Sous-système *distant* (E_D_SITE) (suite)**							
Menaces et vulnérabilités associées	*E_D_ CWHW*	*E_D_ CWSW*	*LAN*	*WAN (dialup)*	*WAN (INET)*	*E_D_ SITE*	*E_D_ USR*	*Commentai-re*
32- Altération du logiciel								
32ML1- Possibilité de modifier ou changer les applicatifs		0,50						
32ML2- Possibilité d'effacer (ou de modifier) des fichiers-programmes		0,75						
32ML3- Possibilité d'être infecté par un virus		0,50						
32S2- facilité de pénétrer les locaux						1,00		
32ML5- facilité de pénétrer le système		0,50						
32RE2- Le réseau permet d'introduire des logiciels malicieux (vers, virus)					0,50			
33- Piégeage du logiciel								
33ML1- Possibilité de créer (ou modifier) des commandes système		0,50						
33ML2- Possibilité d'implanter des programmes pirates		0,75						
33ML3- Possibilité de modifier ou changer les applicatifs		0,50						
33ML4- Possibilité d'existence de fonctions cachée (concep. ou dével.)		0,25						
33ML6- Possibilité d'effacer (ou de modifier) des fichiers-programmes		0,75						
33S2- facilité de pénétrer les locaux						1,00		
33ML7- facilité de pénétrer le système		0,50						
36- Altération des données								
36ML1- Le système permet d'accéder à des données locales	0,00	0,00						
36ML2- Possibilité d'agir sur les données transmises	0,25	0,50						
36RI1- Possibilité d'agir sur les données transmises			0,25					
36RE1- Possibilité d'agir sur les données transmises				0,25	0,25			
36S2- facilité de pénétrer les locaux						1,00		
36ML3- Facilité de pénétrer le système		0,50						
38- Erreur d'utilisation								
38P1- Personnel utilisateur peu ou mal formé							0,50	

ANNEXE 9 - Evaluation des vulnérabilités spécifiques (EBIOS) (suite)

Tableau A9.3	**Sous-système *distant* (E_D_SITE) (suite)**							
Menaces et vulnérabilités associées	*E_D_ CWHW*	*E_D_ CWSW*	*LAN*	*WAN (dialup)*	*WAN (INET)*	*E_D_ SITE*	*E_D_ USR*	*Commentai-re*
40- Usurpation de droits								
40ML1- Le système est connecté à des réseaux externes		0,25						
40ML2- Facilité de pénétrer le système		0,50						
40S2- Facilité de pénétrer les locaux						1,00		

ANNEXE 10 - Evaluation des risques spécifiques (EBIOS)

Tableau A10.1	**Analyse des risques spécifiques pour E_S_SITE**						
MENACES GENERIQUES	*RISQUES SPECIFIQUES*	*D*	*C*	*W*	*I*	*E*	*F/P*
12- PERTE DES TÉLÉCOMMUNICATIONS	**S1- Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)**	**3**					**0,50**
	S2- Destruction accidentelle de la liaison à l"Internet (boucle locale): 12RE2(LLINE)	3					0,25
18- ÉCOUTE PASSIVE	**S3- Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN[100]: 18RI1*18S3**		**3**				**0,50* 0,75**
	S4- Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)		**3**				**0,50**
19- VOL DE SUPPORTS OU DE DOCUMENTS	S5- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe des supports ou des documents: 19S2*19P1		3				0,50* 0,25
20- VOL DE MATÉRIELS	**S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)**	**4**	**3**				**0,50* 0,50**
	S7- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	**3**					**0,50* 0,75**
23- PANNE MATÉRIELLE	**S8- Panne matérielle du serveur du SC: 23ML1(SVHW)**	**4**					**0,25**
	S9- Panne des dispositifs de protection logique: 23ML1(FWHW)	3					0,25
	S10- Panne d'un élément du LAN: 23RI1	3					0,25
24- DYSFONCTIONNEMENT MATÉRIEL	S11- Dysfonctionnement des dispositifs de protection logique: 24ML2(FWHW)	2					0,25
	S12- Dysfonctionnement du serveur du SC: 24ML2(SVHW)	2					0,25
	S13- Dysfonctionnement d'un élément du LAN: 24RI2	2					0,25
25- SATURATION DU MATÉRIEL *(461h)*	S14- Attaque de type DOS depuis l'extérieur et visant les serveurs et/ou le LAN: 25RE2(INET)*25ML1	4					0,50* 0,25
	S15- Attaque de type DOS depuis l'extérieur et visant la connexion WAN: 25RE2(INET)*25RE3(LLINE)	**4**					**0,50* 0,50**
26- DYSFONCTIONNEMENT LOGICIEL	**S16- Erreur de conception, nstallation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)**	**2**	**2**	**2**	**2**	**3**	**0,25**
	S17- Erreur de conception, nstallation et/ou configuration au niveau des serveurs des dispositifs de protection logique: 26ML1/26ML2(FWSW)	2					0,25
31- UTILISATION ILLICITE DU MATÉRIEL	S18- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW et détourne les ressources des logiciels: 31S2*31ML5(SVSW)*31ML3(SVSW)	2	3	3	3	4	0,50* 0,25* 0,25
	S19- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre FWSW et détourne les ressources des logiciels: 31S2*31ML5(FWSW)*31ML3(FWSW)	2	3				0,50* 0,25* 0,25
	S20- Une personne accède à E_S_SITE depuis le WAN(INET), pénètre SVSW et détourne les ressources des logiciels: 31RE1*31ML5(SVSW)*31ML3(SVSW)	2	3	3	3	4	0,25* 0,25* 0,25
	S21- Une personne accède à E_S_SITE depuis le WAN(INET), pénètre FWSW et détourne les ressources des logiciels: 31RE1*31ML5(FWSW)*31ML3(FWSW)	2	3				0,25* 0,25* 0,25
32- ALTÉRATION DU LOGICIEL	S22- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW et modifie les applications ou les fichiers programmes: 32S2*32ML5(SVSW)*32ML1/32ML2(SVSW)	3			4		0,50* 0,25* 0,25
	S23- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre FWSW et modifie les applications ou les fichiers programmes: 32S2*32ML5(FWSW)*32ML1/32ML2(FWSW)	3			4		0,50* 0,25* 0,25
	S24- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW et efface des fichiers-programmes: 32S2*32ML5(SVSW)*32ML2(SVSW)	3			4		0,50* 0,25* 0,50
	S25- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre FWSW et efface des fichiers-programmes: 32S2*32ML5(FWSW)*32ML2(FWSW)	3			4		0,50* 0,25* 0,50
	S26- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(FWSW)	3			4		0,50* 0,25

[100] Comme nous avons exclu l'ajoût de matériel, et à moins d'un enregistrement sur une station locale avec écoute différée, cette écoute aurait lieu en dehors des heures de travail du site E_S_SITE.

ANNEXE 10 - Evaluation des risques spécifiques (EBIOS) (suite)

Tableau A10.1	**Analyse des risques spécifiques pour E_S_SITE (suite)**						
MENACES GENERIQUES	*RISQUES SPECIFIQUES*	*D*	*C*	*W*	*I*	*E*	*F/P*
33- PIÉGEAGE DU LOGICIEL	S27- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW et modifie les applications ou les fichiers programmes: 33S2*33ML7(SVSW)*33ML1/33ML3(SVSW)	2	3	3	4	3	0,50* 0,25* 0,25
	S28- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre FWSW et modifie les applications ou les fichiers programmes: 33S2*33ML7(FWSW)*33ML1/33ML3(FWSW)	2	3	3	4	3	0,50* 0,25* 0,25
	S29- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW et efface ou implante des fichiers-programmes: 33S2*33ML7(SVSW)*33ML2/33ML6(SWSW)	2	3	3	4	3	0,50* 0,25* 0,50
	S30- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre FWSW et efface ou implante des fichiers-programmes: 33S2*33ML7(FWSW)*33ML2/33ML6(FWSW)	2	3	3	4	3	0,50* 0,25* 0,50
36- ALTÉRATION DES DONNÉES	**S31- Une personne extérieure à l'entreprise pénètre E_S_SITE et altère les données transitant sur le LAN: 36S2*36RI1**	**2**	**3**	**3**	**4**		**0,50* 0,25**
	S32- Une personne extérieure à l'entreprise altère les données transitant sur le WAN: 36RE1(INET)	**2**	**3**	**3**	**4**		**0,25**
	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	**2**	**4**	**4**	**4**	**4**	**0,50* 0,25* 0,50**
37- ERREUR DE SAISIE	S34- Erreur de saisie par l'administrateur des catégories d'informations I_PARAMS, I_PROFIL et/ou I_AUTH	2	2	3		4	0,25* 0,25
40- USURPATION DE DROIT	**S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)**	**2**	**2**	**4**	**2**		**0,50* 0,25**
	S36- Une personne extérieure à l'entreprise accède à E_S_SITE depuis le WAN(INET), et pénètre SVSW: 40ML1*40ML2(SVSW/FWSW)	2	2	4	2		0,25* 0,25

ANNEXE 10 - Evaluation des risques spécifiques (EBIOS) (suite)

Tableau A10.2	**Analyse des risques spécifiques pour E_L_SITE**						
MENACES GENERIQUES	*RISQUES SPECIFIQUES*	*D*	*C*	*W*	*I*	*E*	*F/P*
12- PERTE DES TÉLÉCOMMUNICATIONS[101]	L1-						
18- ÉCOUTE PASSIVE[102]	**L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN[103]: 18RI1*18S3**		**2**				**0,75* 0,75**
20- VOL DE MATÉRIELS	**L3- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe tous les postes clients: 20S2*20ML1(CWHW)**	**3**					**0,75* 0,50**
	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	**3**					**0,75* 0,75**
	L5- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe le poste du développeur: 20S2*20ML1	1					0,75* 0,50
	L6- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un poste client: 20S2*20ML1(CWHW)	2					0,75* 0,50
23- PANNE MATÉRIELLE[104]	L7- Panne d'un élément du LAN: 23RI1	2					0,25
24- DYSFONCTIONNEMENT MATÉRIEL	L8- Dysfonctionnement d'un élément du LAN: 24RI2	2					0,25
	L9- Dysfonctionnement d'un poste utilisateur: 23ML1	1					0,25
26- DYSFONCTIONNEMENT LOGICIEL	**L10- Dysfonctionnement logiciel de l'ensemble des postes clients: 26ML1 ou 26ML2**	**1**	**1**	**1**	**1**		**0,25**
31- UTILISATION ILLICITE DU MATÉRIEL	**L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5**	**2**	**1**	**2**			**0,75* 0,50**
32- ALTÉRATION DU LOGICIEL	**L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW/DWSW)**	**2**			**4**		**0,50* 0,50**
	L14- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)	2			4		0,75* 0,50* 0,50
	L15- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre TOUS LES CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	**2**			**4**		**0,75* 0,75* 0,50**
33- PIÉGEAGE DU LOGICIEL	**L16- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)**	**2**	**2**	**2**	**4**		**0,75* 0,50* 0,50**
	L17- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	**2**	**2**	**2**	**4**		**0,75* 0,50* 0,75**
	L18- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre DWSW et y piège le logiciel en phase de développement: 33S2*33ML7(DWSW)*33ML4(DWSW)	**2**	**4**	**3**	**4**	**3**	**0,75* 0,50* 0,50**
36- ALTÉRATION DES DONNÉES	L19- Une personne extérieure à l'entreprise pénètre E_L_SITE et altère les données transitant sur le LAN: 36S2*36RI1	1	2	2	4		0,75* 0,25
38- ERREUR D'UTILISATION	**L20- SC client connecté en l'absence de l'utilisateur: 38P1**	**1**	**2**	**3**			**0,50**
40- USURPATION DE DROIT	**L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)**	**1**	**2**	**3**	**1**		**0,75* 0,50**

[101] Le réseau externe est le même que pour E_S_SITE (voir figure 5.3), où il a déjà été envisagé avec un niveau d'impact plus important.

[102] Le réseau externe est le même que pour E_S_SITE (voir figure 5.3) , où il a déjà été envisagé avec un niveau d'impact plus important.

[103] Comme nous avons exclu l'ajoût de matériel, et à moins d'un enregistrement sur une station locale avec écoute différée, cette écoute aurait lieu en dehors des heures de travail du site E_S_SITE.

[104] Les dispositifs de protection logique sont les mêmes que pour E_S_SITE (voir figure 5.3) , où ils ont déjà été envisagés avec un niveau d'impact plus important.

ANNEXE 10 - Evaluation des risques spécifiques (EBIOS) (suite)

Tableau A10.3	**Analyse des risques spécifiques pour E_D_SITE**						
MENACES GENERIQUES	*RISQUES SPECIFIQUES*	*D*	*C*	*W*	*I*	*E*	*F/P*
12- PERTE DES TÉLÉCOMMUNICATIONS	D1- Destruction accidentelle de la liaison à l"Internet (boucle locale): 12RE2(DIALUP)	1					0,25
18- ÉCOUTE PASSIVE	D2- Une personne extérieure à l'entreprise pénètre E_D_SITE et procède à une écoute passive au niveau du LAN [105] (si présent): 18RI1*18S3		1				0,50* 1,00
20- VOL DE MATÉRIELS	D3- Une personne extérieure à l'entreprise pénètre E_D_SITE et dérobe un poste client: 20S2*20ML1(CWHW)	1					1,00* 0,50
	D4- Une personne extérieure à l'entreprise pénètre E_D_SITE et dérobe un élément du LAN (si présent): 20S2*20RI2(LAN)	1					1,00* 0,75
23- PANNE MATÉRIELLE[106]	D5- Panne matérielle du poste client: 23ML1(CWHW)	1					0,25
	D6- Panne d'un élément du LAN: 23RI1	1					0,25
24- DYSFONCTIONNEMENT MATÉRIEL	D7- Dysfonctionnement d'un élément du LAN: 24RI2	1					0,25
	D8- Dysfonctionnement d'un poste utilisateur: 23ML1	1					0,25
26- DYSFONCTIONNEMENT LOGICIEL	**D9- Dysfonctionnement logiciel du poste client: 26ML1 ou 26ML2**	**1**	**1**	**1**	**1**		**0,25**
31- UTILISATION ILLICITE DU MATÉRIEL	**D10- Consommation abusive des ressources du réseau par l'utilisation des postes clients à des fins non professionnelles: 31ML1 ou 31ML3**	**1**	**1**	**1**			**0,75**
	D11- Une personne extérieure à l'entreprise pénètre E_D_SITE et utilise illicitement le matériel: 31S2*31ML5	1					1,00* 0,50
32- ALTÉRATION DU LOGICIEL	**D12- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW)**	**1**			**4**		**0,75* 0,50**
	D13- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)	**1**			**4**		**1,00* 0,75* 0,50**
	D14- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	**1**			**4**		**1,00* 0,75* 0,75**
33- PIÉGEAGE DU LOGICIEL	**D15- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)**	**1**	**1**		**4**		**1,00* 0,75* 0,50**
	D16- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	**1**	**1**		**4**		**1,00* 0,75* 0,75**
36- ALTÉRATION DES DONNÉES	D17- Une personne extérieure à l'entreprise pénètre E_D_SITE et altère les données transitant sur le LAN: 36S2*36RI1	1		1	3		1,00* 0,25
38- ERREUR D'UTILISATION	**D18- SC client connecté en l'absence de l'utilisateur: 38P1**		**1**	**2**			**0,50**
40- USURPATION DE DROIT	**D19- Une personne extérieure à l'entreprise pénètre E_D_SITE et pénètre CWSW: 40S2*40ML2(CWSW)**	**1**	**2**	**3**			**1,00* 0,75**

105 Comme nous avons exclu l'ajoût de matériel, et à moins d'un enregistrement sur une station locale avec écoute différée, cette écoute aurait lieu en dehors des heures de travail du site E_S_SITE.

[106] Les dispositifs de protection logique sont les mêmes que pour E_S_SITE (voir figure 5.3) , où ils ont déjà été envisagés avec un niveau d'impact plus important.

ANNEXE 11 - Grilles des références croisées entre risques spécifiques et entités du SC

Tableau A11.1	**Références croisées entre risques spécifiques et entités du SC pour E_S_SITE (d'après tableau 5.5 et tableau A9.1, ANNEXE 9)**										
MG	*RISQUES SPECIFIQUES*	*E_S_ SVHW*	*E_S_ FWHW*	*E_S_ SVSW*	*E_S_ FWSW*	*E_S_ INET*	*E_S_ WAN*	*E_S_ LAN*	*E_S_ ADMIN*	*E_S_ SITE*	*E_S_E NTORG*
12	S1- Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)					X					
18	S3- Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3							X		X	
18	S4- Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)					X	X				
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	X								X	
20	S7- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)							X		X	
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	X									
25	S15- Attaque de type DOS depuis l'extérieur et visant la connexion WAN: 25RE2(INET)*25RE3(LLINE)					X	X				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)			X							
36	S31- Une personne extérieure à l'entreprise pénètre E_S_SITE et altère les données transitant sur le LAN: 36S2*36RI1							X		X	
36	S32- Une personne extérieure à l'entreprise altère les données transitant sur le WAN: 36RE1(INET)					X					
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)			X						X	
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)			X						X	

ANNEXE 11 - Grilles des références croisées entre risques spécifiques et entités du SC

Tableau A11.2	**Références croisées entre risques spécifiques et entités du SC pour E_L_SITE (d'après tableau 5.5 et tableau A9.2, ANNEXE 9)**											
MG	*RISQUES SPECIFIQUES*	*E_L_ DWHW*	*E_L_ CWHW*	*E_L_ DWSW*	*E_L_ CWSW*	*E_L_ INET*	*E_L_ WAN*	*E_L_ LAN*	*E_L_ DEV*	*E_L_ USR*	*E_L_ SITE*	*E_L_E NTORG*
18	L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3							X			X	
20	L3- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe tous les postes clients: 20S2*20ML1(CWHW)		X								X	
20	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)							X			X	
26	L10- Dysfonctionnement logiciel de l'ensemble des postes clients: 26ML1 ou 26ML2				X							
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5			X	X						X	
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)			X	X	X						
32	L15- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre TOUS LES CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)				X						X	
33	L16- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)				X						X	
33	L17- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)				X						X	
33	L18- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre DWSW et y piège le logiciel en phase de développement: 33S2*33ML7(DWSW)*33ML4(DWSW)			X								
38	L20- SC client connecté en l'absence de l'utilisateur: 38P1									X		
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)			X	X						X	

ANNEXE 11 - Grilles des références croisées entre risques spécifiques et entités du SC

Tableau A11.2	**Références croisées entre risques spécifiques et entités du SC pour E_D_SITE (d'après tableau 5.5 et tableau A9.3, ANNEXE 9)**									
MG	*RISQUES SPECIFIQUES*	*E_D_CWHW*	*E_D_CWSW*	*E_D_INET*	*E_D_WAN*	*E_D_LAN*	*E_D_USR*	*E_D_SITE*	*E_D_CLIORG*	*E_D_ENTORG*
26	D9- Dysfonctionnement logiciel du poste client: 26ML1 ou 26ML2		X							
31	D10- Consommation abusive des ressources du réseau par l'utilisation des postes clients à des fins non professionnelles: 31ML1 ou 31ML3		X			X				
32	D12- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW)		X	X						
32	D13- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)		X					X		
32	D14- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)		X					X		
33	D15- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)		X					X		
33	D16- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)		X					X		
38	D18- SC client connecté en l'absence de l'utilisateur: 38P1						X			
40	D19- Une personne extérieure à l'entreprise pénètre E_D_SITE et pénètre CWSW: 40S2*40ML2(CWSW)		X					X		

ANNEXE 12 - Fiches de confrontation des risques aux besoins

Tableau A12.1	**Fiche de confrontation des menaces aux besoins**										
Fonction:	*F_COMM*					*Sensibilité*				
Catégorie d'information:						*D*	*C*	*W*	*I*	*E*
						2		*3*		*4*
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
12	S1- Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)	3					**2**				
18	S3- Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		3								
18	S4- Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)		3								
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	4	3				**2**				
20	S7- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	4					**2**				
25	S15- Attaque de type DOS depuis l'extérieur et visant la connexion WAN: 25RE2(INET)*25RE3(LLINE)	4					**2**				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**2**		**3**		**4**
36	S31- Une personne extérieure à l'entreprise pénètre E_S_SITE et altère les données transitant sur le LAN: 36S2*36RI1	2	3	3	4		**2**		**3**		
36	S32- Une personne extérieure à l'entreprise altère les données transitant sur le WAN: 36RE1(INET)	2	3	3	4		**2**		**3**		
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**2**		**3**		**4**
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**2**		**3**		
	E_L_SITE										
18	L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		2								
20	L3- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe tous les postes clients: 20S2*20ML1(CWHW)	3					**2**				
20	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
26	L10- Dysfonctionnement logiciel de l'ensemble des postes clients: 26ML1 ou 26ML2	1	1	1	1		**2**		**3**		
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5	2	1	2			**2**		**3**		
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)	2			4		**2**				
32	L15- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre TOUS LES CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	2			4		**2**				
33	L16- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	2	2	2	4		**2**		**3**		
33	L17- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	2	2	2	4		**2**		**3**		
38	L20- SC client connecté en l'absence de l'utilisateur: 38P1	1	2	3			**2**		**3**		
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)	1	2	3	1		**2**		**3**		
	E_D_SITE										
26	D9- Dysfonctionnement logiciel du poste client: 26ML1 ou 26ML2	1	1	1	1		**2**		**3**		
31	D10- Consommation abusive des ressources du réseau par l'utilisation des postes clients à des fins non professionnelles: 31ML1 ou 31ML3	1	1	1			**2**		**3**		
32	D12- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW)	1			4		**2**				

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.1 (suite)	**Fiche de confrontation des menaces aux besoins**										
Fonction:	*F_COMM*					*Sensibilité*				
Catégorie d'information:						*D*	*C*	*W*	*I*	*E*
						2		*3*		*4*
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_D_SITE (suite)										
32	D13- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)	1			4		**2**				
32	D14- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	1			4		**2**				
33	D15- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	1	1		4		**2**				
33	D16- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	1	1		4		**2**				
38	D18- SC client connecté en l'absence de l'utilisateur: 38P1		1	2					**3**		
40	D19- Une personne extérieure à l'entreprise pénètre E_D_SITE et pénètre CWSW: 40S2*40ML2(CWSW)	1	2	3			**2**		**3**		

Tableau A12.2	**Fiche de confrontation des menaces aux besoins**										
Fonction:	*F_ENROL*					*Sensibilité*				
Catégorie d'information:						*D*	*C*	*W*	*I*	*E*
						1		*3*		*2*
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	4	3				**1**				
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	4					**1**				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**1**		**3**		**2**
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**1**		**3**		**2**
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**1**		**3**		**2**

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.3	**Fiche de confrontation des risques aux besoins**										
Fonction:	*F_DEVEL*					*Sensibilité*				
Catégorie d'information:						*D*	*C*	*W*	*I*	*E*
						1		*3*		*2*
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_L_SITE										
18	L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		2								
20	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					1				
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5	2	1	2			1		3		
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)	2			4		1				
33	L18- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre DWSW et y piège le logiciel en phase de développement: 33S2*33ML7(DWSW)*33ML4(DWSW)	2	4	3	4	3	1		3		2
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)	1	2	3	1		1		3		

Tableau A12.4	**Fiche de confrontation des risques aux besoins**										
Fonction:	*F_DEPLO*					*Sensibilité*				
Catégorie d'information:						*D*	*C*	*W*	*I*	*E*
						1				*4*
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
12	S1- Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)	3					1				
18	S3- Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		3								
18	S4- Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)		3								
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	4	3				1				
20	S7- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					1				
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	4					1				
25	S15- Attaque de type DOS depuis l'extérieur et visant la connexion WAN: 25RE2(INET)*25RE3(LLINE)	4					1				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	1				4
36	S31- Une personne extérieure à l'entreprise pénètre E_S_SITE et altère les données transitant sur le LAN: 36S2*36RI1	2	3	3	4		1				
36	S32- Une personne extérieure à l'entreprise altère les données transitant sur le WAN: 36RE1(INET)	2	3	3	4		1				
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	1				4
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		1				
	E_L_SITE										
18	L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		2								
20	L3- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe tous les postes clients: 20S2*20ML1(CWHW)	3					1				

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.4 (suite)	**Fiche de confrontation des risques aux besoins**										
Fonction:	*F_DEPLO*						*Sensibilité*				
Catégorie d'information:							*D*	*C*	*W*	*I*	*E*
							1				*4*
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_L_SITE (suite)										
20	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3									
26	L10- Dysfonctionnement logiciel de l'ensemble des postes clients: 26ML1 ou 26ML2	1	1	1	1		**1**				
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5	2	1	2			**1**				
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)	2			4		**1**				
32	L15- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre TOUS LES CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	2			4		**1**				
33	L16- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	2	2	2	4		**1**				
33	L17- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	2	2	2	4		**1**				
33	L18- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre DWSW et y piège le logiciel en phase de développement: 33S2*33ML7(DWSW)*33ML4(DWSW)	2	4	3	4	3	**1**				**4**
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)	1	2	3	1		**1**				
	E_D_SITE										
26	D9- Dysfonctionnement logiciel du poste client: 26ML1 ou 26ML2	1	1	1	1		**1**				
31	D10- Consommation abusive des ressources du réseau par l'utilisation des postes clients à des fins non professionnelles: 31ML1 ou 31ML3	1	1	1			**1**				
32	D12- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW)	1			4		**1**				
32	D13- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)	1			4		**1**				
32	D14- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	1			4		**1**				
33	D15- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	1	1		4		**1**				
33	D16- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	1	1		4		**1**				
40	D19- Une personne extérieure à l'entreprise pénètre E_D_SITE et pénètre CWSW: 40S2*40ML2(CWSW)	1	2	3			**1**				

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.5	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_AUTH*						*D*	*C*	*W*	*I*	*E*
							2	*3*	*3*	*3*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	4	3				**2**	**3**			
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	4					**2**				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**2**	**3**	**3**	**3**	
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**2**	**3**	**3**	**3**	
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**2**	**3**	**3**		
	E_L_SITE										
38	L20- SC client connecté en l'absence de l'utilisateur: 38P1	1	2	3			**2**	**3**			
	E_D_SITE										
38	D18- SC client connecté en l'absence de l'utilisateur: 38P1		1	2				**3**	**3**		

Tableau A12.6	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_PROFIL*						*D*	*C*	*W*	*I*	*E*
							2	*2*	*2*	*2*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
12	S1- Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)	3					**2**				
18	S3- Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		3					**2**			
18	S4- Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)		3					**2**			
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	4	3				**2**	**2**			
20	S7- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	4					**2**				
25	S15- Attaque de type DOS depuis l'extérieur et visant la connexion WAN: 25RE2(INET)*25RE3(LLINE)	4					**2**				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**2**	**2**	**2**	**2**	
36	S31- Une personne extérieure à l'entreprise pénètre E_S_SITE et altère les données transitant sur le LAN: 36S2*36RI1	2	3	3	4		**2**	**2**	**2**	**2**	
36	S32- Une personne extérieure à l'entreprise altère les données transitant sur le WAN: 36RE1(INET)	2	3	3	4		**2**	**2**	**2**	**2**	
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**2**	**2**	**2**	**2**	
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**2**	**2**	**2**	**2**	

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.6 (suite)	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_PROFIL*						*D*	*C*	*W*	*I*	*E*
							2	*2*	*2*	*2*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_L_SITE										
18	L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		2					**2**			
20	L3- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe tous les postes clients: 20S2*20ML1(CWHW)	3					**2**				
20	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
26	L10- Dysfonctionnement logiciel de l'ensemble des postes clients: 26ML1 ou 26ML2	1	1	1	1		**2**	**2**	**2**	**2**	
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5	2	1	2			**2**	**2**	**2**		
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)	2			4		**2**			**2**	
32	L15- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre TOUS LES CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	2			4		**2**			**2**	
33	L16- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	2	2	2	4		**2**	**2**	**2**	**2**	
33	L17- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	2	2	2	4		**2**	**2**	**2**	**2**	
38	L20- SC client connecté en l'absence de l'utilisateur: 38P1	1	2	3			**2**	**2**	**2**		
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)	1	2	3	1		**2**	**2**	**2**	**2**	
	E_D_SITE										
26	D9- Dysfonctionnement logiciel du poste client: 26ML1 ou 26ML2	1	1	1	1		**2**	**2**	**2**	**2**	
31	D10- Consommation abusive des ressources du réseau par l'utilisation des postes clients à des fins non professionnelles: 31ML1 ou 31ML3	1	1	1			**2**	**2**	**2**		
32	D12- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW)	1			4		**2**			**2**	
32	D13- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)	1			4		**2**			**2**	
32	D14- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	1			4		**2**			**2**	
33	D15- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	1	1		4		**2**	**2**		**2**	
33	D16- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	1	1		4		**2**	**2**		**2**	
38	D18- SC client connecté en l'absence de l'utilisateur: 38P1		1	2				**2**	**2**		

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.7	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_COMM*						*D*	*C*	*W*	*I*	*E*
							2	*3*	*3*	*2*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
12	S1- Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)	3					**2**				
18	S3- Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		3					**3**			
18	S4- Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)		3					**3**			
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	4	3				**2**	**3**			
20	S7- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	4					**2**				
25	S15- Attaque de type DOS depuis l'extérieur et visant la connexion WAN: 25RE2(INET)*25RE3(LLINE)	4					**2**				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**2**	**3**	**3**	**2**	
36	S31- Une personne extérieure à l'entreprise pénètre E_S_SITE et altère les données transitant sur le LAN: 36S2*36RI1	2	3	3	4		**2**	**3**	**3**	**2**	
36	S32- Une personne extérieure à l'entreprise altère les données transitant sur le WAN: 36RE1(INET)	2	3	3	4		**2**	**3**	**3**	**2**	
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**2**	**3**	**3**	**2**	
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**2**	**3**	**3**	**2**	
	E_L_SITE										
18	L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		2					**3**			
20	L3- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe tous les postes clients: 20S2*20ML1(CWHW)	3					**2**				
20	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
26	L10- Dysfonctionnement logiciel de l'ensemble des postes clients: 26ML1 ou 26ML2	1	1	1	1		**2**	**3**	**3**	**2**	
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5	2	1	2			**2**	**3**	**3**		
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)	2			4		**2**			**2**	
32	L15- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre TOUS LES CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	2			4		**2**			**2**	
33	L16- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	2	2	2	4		**2**	**3**	**3**	**2**	
33	L17- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	2	2	2	4		**2**	**3**	**3**	**2**	
38	L20- SC client connecté en l'absence de l'utilisateur: 38P1	1	2	3			**2**	**3**	**3**		
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)	1	2	3	1		**2**	**3**	**3**	**2**	

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.7 (suite)	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_COMM*						*D*	*C*	*W*	*I*	*E*
							2	*3*	*3*	*2*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_D_SITE										
26	D9- Dysfonctionnement logiciel du poste client: 26ML1 ou 26ML2	1	1	1	1		**2**	**3**	**3**		
31	D10- Consommation abusive des ressources du réseau par l'utilisation des postes clients à des fins non professionnelles: 31ML1 ou 31ML3	1	1	1			**2**	**3**	**3**		
32	D12- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW)	1			4		**2**			**2**	
32	D13- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)	1			4		**2**			**2**	
32	D14- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	1			4		**2**			**2**	
33	D15- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	1	1		4		**2**	**3**		**2**	
33	D16- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	1	1		4		**2**	**3**		**2**	
38	D18- SC client connecté en l'absence de l'utilisateur: 38P1		1	2				**3**	**3**		
40	D19- Une personne extérieure à l'entreprise pénètre E_D_SITE et pénètre CWSW: 40S2*40ML2(CWSW)	1	2	3			**2**	**3**	**3**		

Tableau A12.8	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_CODSRC*						*D*	*C*	*W*	*I*	*E*
							2		*3*	*3*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_L_SITE										
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5	2	1	2			**2**	**3**	**3**		
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)	2			4		**2**			**2**	
33	L18- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre DWSW et y piège le logiciel en phase de développement: 33S2*33ML7(DWSW)*33ML4(DWSW)	2	4	3	4	3	**2**	**3**	**3**	**2**	
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)	1	2	3	1		**2**	**3**	**3**	**2**	

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.9	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_CODBIN*						*D*	*C*	*W*	*I*	*E*
							2		*2*	*2*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
12	S1- Défaillances graves dans le fonctionnement et les performances de l'Internet: 12RE1(INET)	3					**2**				
18	S3- Une personne extérieure à l'entreprise pénètre E_S_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		3								
18	S4- Une personne extérieure à l'entreprise procède à une écoute passive au niveau du WAN (INET): 18RE1(INET)		3								
20	S6- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe le serveur d'application: 20S2*20ML1(SVHW)	4	3				**2**				
20	S7- Une personne extérieure à l'entreprise pénètre E_S_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
23	S8- Panne matérielle du serveur du SC: 23ML1(SVHW)	4					**2**				
25	S15- Attaque de type DOS depuis l'extérieur et visant la connexion WAN: 25RE2(INET)*25RE3(LLINE)	4					**2**				
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**2**		**2**	**2**	
36	S31- Une personne extérieure à l'entreprise pénètre E_S_SITE et altère les données transitant sur le LAN: 36S2*36RI1	2	3	3	4		**2**		**2**	**2**	
36	S32- Une personne extérieure à l'entreprise altère les données transitant sur le WAN: 36RE1(INET)	2	3	3	4		**2**		**2**	**2**	
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**2**		**2**	**2**	
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**2**		**2**	**2**	
	E_L_SITE										
18	L2- Une personne extérieure à l'entreprise pénètre E_L_SITE et procède à une écoute passive au niveau du LAN: 18RI1*18S3		2								
20	L3- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe tous les postes clients: 20S2*20ML1(CWHW)	3					**2**				
20	L4- Une personne extérieure à l'entreprise pénètre E_L_SITE et dérobe un élément du LAN: 20S2*20RI2(LAN)	3					**2**				
26	L10- Dysfonctionnement logiciel de l'ensemble des postes clients: 26ML1 ou 26ML2	1	1	1	1		**2**		**2**	**2**	
31	L12- Une personne extérieure à l'entreprise pénètre E_L_SITE et utilise illicitement le matériel: 31S2*31ML5	2	1	2			**2**		**2**		
32	L13- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(DWSW/CWSW)	2			4		**2**			**2**	
32	L15- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre TOUS LES CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	2			4		**2**			**2**	
33	L16- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	2	2	2	4		**2**		**2**	**2**	
33	L17- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre tous les CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	2	2	2	4		**2**		**2**	**2**	
33	L18- Une personne extérieure à l'entreprise pénètre E_L_SITE , pénètre DWSW et y piège le logiciel en phase de développement: 33S2*33ML7(DWSW)*33ML4(DWSW)	2	4	3	4	3	**2**		**2**	**2**	
40	L21- Une personne extérieure à l'entreprise pénètre E_L_SITE et pénètre CWSW/DWSW: 40S2*40ML2(CWSW/DWSW)	1	2	3	1		**2**		**2**	**2**	

ANNEXE 12 - Fiches de confrontation des risques aux besoins (suite)

Tableau A12.9 (suite)	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_CODBIN*						*D*	*C*	*W*	*I*	*E*
							2		*2*	*2*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_D_SITE										
26	D9- Dysfonctionnement logiciel du poste client: 26ML1 ou 26ML2	1	1	1	1		**2**		**2**	**2**	
31	D10- Consommation abusive des ressources du réseau par l'utilisation des postes clients à des fins non professionnelles: 31ML1 ou 31ML3	1	1	1			**2**		**2**		
32	D12- Le réseau externe permet d'introduire des vers ou des virus: 32RE2(INET)*32ML3(CWSW)	1			4		**2**			**2**	
32	D13- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y modifie des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML1/32ML2(CWSW)	1			4		**2**			**2**	
32	D14- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y efface des applications ou des fichiers programmes: 32S2*32ML5(CWSW)*32ML2(CWSW)	1			4		**2**			**2**	
33	D15- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y piège les applications ou les fichiers programmes: 33S2*33ML7(CWSW)*33ML1/33ML3(CWSW)	1	1		4		**2**			**2**	
33	D16- Une personne extérieure à l'entreprise pénètre E_D_SITE , pénètre le CWSW et y implante des programmes pirates: 33S2*33ML7(CWSW)*33ML2(CWSW)	1	1		4		**2**			**2**	
40	D19- Une personne extérieure à l'entreprise pénètre E_D_SITE et pénètre CWSW: 40S2*40ML2(CWSW)	1	2	3			**2**		**2**		

Tableau A12.10	**Fiche de confrontation des risques aux besoins**										
Fonction:							*Sensibilité*				
Catégorie d'information:	*I_PARAM*						*D*	*C*	*W*	*I*	*E*
							2		*3*	*3*	
		Sévérité					*Impact réel*				
MG	*Description*	*D*	*C*	*W*	*I*	*E*	*D*	*C*	*W*	*I*	*E*
	E_S_SITE										
26	S16- Erreur de conception, installation et/ou configuration au niveau du serveur du SC: 26ML1/26ML2(SVSW)	2	2	2	2	3	**2**		**3**	**3**	
36	S33- Une personne extérieure à l'entreprise pénètre E_S_SITE , pénètre SVSW altère les données (locales et transmises): 36S2*36ML3(SVSW)*36ML1(SWSW)	2	4	4	4	4	**2**		**3**	**3**	
40	S35- Une personne extérieure à l'entreprise pénètre E_S_SITE et pénètre SVSW: 40S2*40ML2(SVSW/FWSW)	2	2	4	2		**2**		**3**	**3**	

ANNEXE 13 - Classe de fonctionnalité F-C2 (ITSEC)

Classe de fonctionnalité F-C2

Objectif

L'exemple de classe F-C2 est dérivé des exigences fonctionnelles de la classe C2 du TCSEC américain. Elle offre un contrôle d'accès discrétionnaire plus fin que la classe C1, en rendant les utilisateurs individuellement responsables de leurs actions à travers des procédures d'identification, l'audit des événements relatifs à la sécurité et l'isolation des ressources.

Identification et authentification

La TOE doit identifier et authentifier de **façon unique** les utilisateurs. L'identification et l'authentification doivent avoir lieu avant toute autre interaction entre la TOE et l'utilisateur. D'autres interactions ne doivent être possibles qu'après une identification et une authentification réussies. Les informations d'authentification doivent être stockées de façon telle qu'elles soient seulement accessibles par des utilisateurs autorisés. **Pour chaque interaction, la TOE doit pouvoir établir l'identité de l'utilisateur**.

Contrôle d'accès

La TOE doit pouvoir distinguer et administrer les droits d'accès de chaque utilisateur sur les objets soumis à l'administration des droits, au niveau d'un utilisateur individuel, au niveau de l'appartenance à un groupe d'utilisateurs, ou aux deux niveaux. Il doit être possible de refuser complètement à des utilisateurs ou à des groupes d'utilisateurs l'accès à un objet. **Il doit également être possible de limiter l'accès d'un utilisateur à un objet aux seules opérations qui ne modifient pas cet objet. Il doit être possible d'accorder les droits d'accès à un objet en descendant jusqu'au niveau de granularité de l'utilisateur individuel**. Il ne doit pas être possible à quelqu'un qui n'est pas un utilisateur autorisé d'accorder ou de retirer des droits d'accès à un objet. **L'administration des droits doit disposer de contrôles pour limiter la propagation des droits d'accès. De même, seuls des utilisateurs autorisés doivent pouvoir introduire de nouveaux utilisateurs, supprimer ou suspendre des utilisateurs existants.**

Lors de toute tentative par des utilisateurs ou des groupes d'utilisateurs d'accéder à des objets soumis à l'administration des droits, la TOE doit vérifier la validité de la demande. Les tentatives d'accès non autorisé doivent être rejetées.

Imputabilité

La TOE doit comporter un composant d'imputation qui soit capable, pour chacun des événements suivants, d'enregistrer cet événement avec les données exigées :

a) Utilisation du mécanisme d'identification et d'authentification :

Données exigées : Date ; heure ; identité fournie par l'utilisateur ; identification de l'équipement sur lequel le mécanisme d'identification et d'authentification a été utilisé (par exemple identificateur du terminal) ; réussite ou échec de la tentative.

b) Actions qui tentent d'exercer des droits d'accès à un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de la tentative d'accès ; réussite ou échec de la tentative.

c) Création ou suppression d'un objet soumis à l'administration des droits :

Données exigées : Date ; heure ; identité de l'utilisateur ; nom de l'objet ; type de l'action.

ANNEXE 13 - Classe de fonctionnalité F-C2 (ITSEC) (suite)

d) Actions d'utilisateurs autorisés affectant la sécurité de la TOE :

Données exigées : Date ; heure ; identité de l'utilisateur ; type de l'action ; nom de l'objet sur lequel porte l'action (de telles actions sont l'introduction ou la suppression (suspension) d'utilisateurs ; l'introduction ou le retrait de supports de stockage ; le démarrage ou l'arrêt de la TOE).

Les utilisateurs non autorisés ne doivent pas avoir accès aux données d'imputation. Il doit être possible de mettre sélectivement en oeuvre l'imputation pour un ou plusieurs utilisateurs. Il doit exister des outils pour examiner et maintenir les fichiers d'imputation et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Audit

Il doit exister des outils pour examiner les fichiers d'imputation pour les besoins d'audit et ces outils doivent être documentés. Ils doivent permettre d'identifier sélectivement les actions d'un ou de plusieurs utilisateurs.

Réutilisation d'objet

Tous les objets de stockage rendus à la TOE doivent, avant d'être réutilisés par d'autres sujets, être traités d'une manière telle qu'aucune conclusion ne puisse être tirée concernant leur contenu précédent.

ANNEXE 14 - Programme d'analyse des RTT

```
#include <stdio.h>
#include <stdlib.h>
#include <malloc.h>

#define FALSE   0
#define TRUE    (!FALSE)
#define True    TRUE
#define False   FALSE
#define BBOOL   int

FILE*   Source;

void processRtt(double);
void reportResults(char*);

int count = 0, maxCount = 0, classe = 0, classCount = 0;
double sumRtt = 0.0, maxRtt = 0.0;
double minRtt = 1000.0;

struct tagTCell {
      int           classe;
      int           count;
      char*         prevCell;
      char*         nextCell;
      } ;
typedef struct tagTCell* TCell;
TCell   headList = 0;

TCell  TListFindCell        (TCell tcFrom);
TCell  TListCreateCell      (void);
TCell  TListInsertCell      (TCell tcPrev, TCell tc, TCell tcNew);

main(argc,argv)
int    argc;
char*  argv[];
{

char buffer[10];

      if (argc != 2) {
        printf ("%s\n","Invalide number of arguments (file name required).");
        exit(1);
        }

      if ((Source = fopen (argv[1],"r")) == NULL) {
        printf ("%s\n","The file was not found: %s", argv[1]);
        exit(2);
        }

      while ((fscanf(Source,"%s",buffer)) != EOF)
            processRtt(atof(buffer));

      reportResults(argv[1]);
      fclose(Source);
}
```

ANNEXE 14 - Programme d'analyse des RTT (suite)

```
void processRtt(double rtt) {

TCell tc = headList;
TCell tcSelected = 0;

count++;
sumRtt=sumRtt+rtt;
classe=(int)rtt;
if (minRtt > rtt) minRtt = rtt;
if (maxRtt < rtt) maxRtt = rtt;

//    get the matching cell

//printf("Start processing for class %d\n",classe);
tcSelected = (TCell) TListFindCell (tc);
tcSelected->count++;
if (maxCount < tcSelected->count) maxCount = tcSelected->count;

// printf ("%d\t%f\trounded to %d\n",++count,rtt,(int)(rtt));

}

TCell  TListCreateCell(void) {
TCell  tc = 0;

  if (!(BBOOL)(tc = calloc(sizeof(struct tagTCell),1)))
      return FALSE;
//printf(" New cell created for class %d\n",classe);
  tc->classe = classe;
  tc->count = 0;
  tc->prevCell = 0;
  tc->nextCell = 0;
  classCount++;
  return tc;

}

TCell   TListFindCell (TCell tc) {
TCell   tcPrev = 0, tcNew = 0;

  if (!(BBOOL)(tc)) {          //    list is empty
//printf(" List is empty\n");
      tc=TListCreateCell();
      headList=tc;
      return tc;
      }
```

ANNEXE 14 - Programme d'analyse des RTT (suite)

```
 while (((BBOOL)(tc)) && (!(tc->classe > classe))) {
//printf(" .skipped a cell for class %d\n",tc->classe);
     if (tc->classe == classe) {
//printf(" MATCH\n");
          return tc;
          }
     if (tc->classe < classe) {
          tcPrev = tc;
          tc = (TCell) tc->nextCell;
     }
 }

 tcNew=TListCreateCell();
 TListInsertCell(tcPrev, tc, tcNew);
 return tcNew;
}

TCell  TListInsertCell (TCell tcPrev, TCell tc, TCell tcNew) {

 // insert tcNew after tcPrev and before tc

 if ((BBOOL) (tcPrev)) {     //     tcNew is not the first cell
     tcNew->prevCell      =     (char*) tcPrev;
     tcPrev->nextCell     =     (char*) tcNew;
//printf(" New cell inserted after cell for class %d\n",tcPrev->classe);
     }
 else {
     headList=tcNew;
//printf (" New cell inserted at head of list\n");
     }
 if ((BBOOL) (tc))    {     //     tcNew is not the last cell
     tcNew->nextCell =     (char*) tc;
     tc->prevCell    =     (char*) tcNew;
//printf(" New cell inserted before cell for class %d\n",tc->classe);
     }
 else {
//printf (" New cell inserted at tail of list\n");
     }
}

void reportResults(char* fileName) {
TCell tc;
int subTotal = 0;
```

ANNEXE 14 - Programme d'analyse des RTT (suite)

```
printf("\nAnalysis report for %s\n", fileName);
printf("Nombre de donnees lues: %d\n", count);
printf("Nombre de classes creees: %d\n", classCount);
printf("Moyenne des donnees lues: %f\n", (sumRtt/count));
printf("RTT minimum mesure: %f\n", minRtt);
printf("RTT maximum mesure: %f\n\n", maxRtt);
printf("Distribution:\n");
printf("Classe\tCount\tSubtotal\tPercentile\n");
tc = headList;
while ((BBOOL) (tc)) {
      subTotal=subTotal+tc->count;
      printf("%d\t%d\t%d\t\t%d\n",tc->classe, tc->count, subTotal,
        (100*subTotal/count));
      tc = (TCell) tc->nextCell;
      }
}
```

ANNEXE 15 - Fondements théoriques de la signature biométrique de la frappe au clavier

Cette annexe reproduit, avec l'aimable autorisation de l'auteur, le paragraphe 5.6 de [Philippe-02].

Définition

L'encodage au clavier d'un texte T composé de n caractères peut être découpé en différents types d'événements, parmi ceux-ci nous distinguons :

- Le début de la saisie du texte T ;
- Le début de pression d'une touche particulière k ;
- La fin de pression d'une touche particulière k ;
- La fin de saisie du texte T.

Chaque événement se produisant à un instant t.

Ainsi la saisie du texte T = « *daniel* » pourrait être découpée en événements de la manière suivante.

Evénement	Instant (ms)
Début de saisie du texte	0
Début de pression de la touche *d*	0
Fin de pression de la touche *d*	57
Début de pression de la touche *a*	111
Fin de pression de la touche *a*	180
Début de pression de la touche *n*	226
Début de pression de la touche *i*	260
Fin de pression de la touche *n*	280
Fin de pression de la touche *i*	290
Début de pression de la touche *e*	350
Fin de pression de la touche *e*	395
Début de pression de la touche *l*	420
Fin de pression de la touche *l*	450
Fin de saisie du texte	450

Dans notre prototype, nous avons choisi de définir la signature biométrique S d'ordre n correspondant à l'encodage du texte T comme étant un ensemble de n couples ($downtime_i$, $interdowntime_i$), donc :

$$S = [(downtime_1, interdowntime_1);...;(downtime_n, interdowntime_n)]$$

Où :

- $downtime_i$ représente le temps de pression, exprimé en millisecondes (ms), de la touche correspondant au caractère occupant la position i dans le texte T;
- $interdowntime_i$ représente le temps, exprimé en millisecondes, écoulé entre le début de la pression de la touche correspondant au caractère occupant la position $(i-1)$ et le début de la pression de la touche correspondant au caractère occupant la position i dans le texte T pour i > 1. Nous donnerons la valeur 0 à $interdowntime_1$.

Construisons maintenant la signature propre à notre exemple précédent :

Position (*i*)	Caractère	Downtime (ms)	Interdowntime (ms)
1	*D*	57 – 0 = 57	0
2	*A*	180 – 111 = 69	111 – 0 = 111
3	*N*	280 – 226 = 54	226 – 111 = 115
4	*I*	290 – 260 = 30	260 – 226 = 34
5	*E*	395 – 350 = 45	350 – 260 = 90
6	*L*	450 – 420 = 30	420 – 350 = 70

ANNEXE 15 - Fondements théoriques de la signature biométrique de la frappe au clavier (suite)

Cette annexe reproduit, avec l'aimable autorisation de l'auteur, le paragraphe 5.6 de [Philippe-02].

Soit S = [(57,0) ; (69,111) ; (54,115) ; (30,34) ; (45, 90) ; (30, 70)]

Durée totale

Soit A une signature biométrique d'ordre n

Définissons *durée_totale(A)* comme étant un réel égal à

$$durée\_totale(A) = A.downtime_n + \sum_{i=1}^{n} A.interdowntime_i$$

La durée totale d'une signature biométrique du texte T correspond au temps écoulé entre la pression de la touche correspondant au premier caractère de T et le lâcher de la touche correspondant au dernier caractère de T.

Addition

Soit A une signature biométrique d'ordre n
Soit B une signature biométrique d'ordre n

Définissons $C = A + B$ comme étant une signature biométrique d'ordre n égale à

$$C = [\ (A.downtime_1 + B.downtime_1,\ A.interdowntime_1 + B.interdowntime_1)\ ;\ \ldots\ ;\ (A.downtime_n + B.downtime_n,\ A.interdowntime_n + B.interdowntime_n)\ ]$$

Soustraction

Soit A une signature biométrique d'ordre n
Soit B une signature biométrique d'ordre n

Définissons $C = A - B$ comme étant une signature biométrique d'ordre n égale à

$$C = [\ (A.downtime_1 - B.downtime_1,\ A.interdowntime_1 - B.interdowntime_1)\ ;\ \ldots\ ;\ (A.downtime_n - B.downtime_n,\ A.interdowntime_n - B.interdowntime_n)\ ]$$

Division par un réel

Soit A une signature biométrique d'ordre n
Soit r un réel tel que $r \neq 0$

Définissons $B = \frac{A}{r}$ comme étant une signature biométrique d'ordre n égale à

$$B = \left[\left(\frac{A.downtime_1}{r}, \frac{A.interdowntime_1}{r} \right); \ldots; \left(\frac{A.downtime_n}{r}, \frac{A.interdowntime_n}{r} \right) \right]$$

ANNEXE 15 - Fondements théoriques de la signature biométrique de la frappe au clavier (suite)

Cette annexe reproduit, avec l'aimable autorisation de l'auteur, le paragraphe 5.6 de [Philippe-02].

Distance

Soit *A* une signature biométrique d'ordre *n*
Soit *B* une signature biométrique d'ordre *n*

Définissons *distance(A,B)* comme étant le réel égal à

$$distance(A,B) = \sum_{i=1}^{n} \sqrt{(A.downtime_i - B.downtime_i)^2 + (A.interdowntime_i - B.interdowntime_i)^2}$$

Nous définissons donc la distance entre deux signatures biométriques comme étant la somme des distances euclidiennes entre les n couples de A et B de même indice.

Distance moyenne

Soit *A* une signature biométrique d'ordre *n*
Soit *B* une signature biométrique d'ordre *n*

Définissons *distance_moyenne(A,B)* comme étant le réel égal à

$$distance\_moyenne(A,B) = \frac{distance(A,B)}{n}$$

Distance relative

Soit *A* une signature biométrique d'ordre *n*
Soit *B* une signature biométrique d'ordre *n*

Définissons *distance_relative(A,B)* comme étant le réel égal à

$$distance\_relative(A,B) = \frac{distance(A,B)}{durée\_totale(B)}$$

Moyenne

Soit $A_1, \ldots, A_p$ un ensemble de p signatures biométriques d'ordre n.

Définissons $M = moyenne(A_1, \ldots, A_p)$ comme étant une signature biométrique d'ordre n égale à

$$M = \frac{\sum_{i=1}^{p} Ai}{p}$$

ANNEXE 15 - Fondements théoriques de la signature biométrique de la frappe au clavier (suite)

Cette annexe reproduit, avec l'aimable autorisation de l'auteur, le paragraphe 5.6 de [Philippe-02].

Moyenne2 ou moyenne sans extrêmes

Soit $A_1, \ldots, A_p$ un ensemble de $p > 2$ signatures biométriques d'ordre n *et* $M = moyenne(A_1, \ldots, A_p)$
Tels que $distance(A_1,M) >= distance(A_2,M) >= \ldots >= distance(A_p, M)$

Définissons $M' = moyenne2(A_1, \ldots, A_p)$ comme étant une signature biométrique d'ordre n égale à

$$M' = \frac{\sum_{i=3}^{p} Ai}{p-2}$$

ANNEXE 16 - Signature biométrique de la frappe au clavier: population statistique utilisée

Population constituée de 155 échantillons d'une chaîne composée de 15 caractères. Ces échantillons ont chacun été prélevés à 10H30 (AM), 16H30 (PM) ou 22H30 (EV).
A chaque caractère correspond une durée d'intervale (IDT) et une durée de pression (DT).

Tableau A16.1 Population statistique utilisée

W#	Ech#	AM	PM	EV	K1		K2		K3		K4		K5		K6		K7		K8		K9		K10		K11		K12		K13		K14		K15	
					IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT
52/02	1	1			0	71	171	80	210	80	180	80	180	71	231	70	220	50	160	80	181	70	210	70	160	80	761	80	211	70	170	80	150	80
52/02	2		1		0	60	170	80	230	71	191	60	140	90	200	70	221	60	140	80	180	70	160	70	180	71	141	50	150	70	170	60	160	60
52/02	3	1			0	70	170	70	190	60	241	80	290	50	200	70	191	50	210	60	230	60	151	60	120	80	160	60	120	70	210	60	151	80
1/03	4		1		0	70	180	70	220	70	130	61	141	70	250	80	411	50	140	60	270	50	120	60	141	70	90	60	160	60	120	60	150	70
1/03	5		1		0	90	181	80	220	70	110	70	180	60	90	81	191	80	160	60	170	70	120	70	131	90	110	80	150	80	150	70	140	90
1/03	6		1		0	50	130	80	191	90	190	70	130	80	130	90	211	60	110	80	160	60	140	70	90	90	140	81	121	80	170	70	140	80
2/03	7	1			0	80	190	70	210	71	131	60	170	60	100	100	220	70	111	70	250	60	110	70	150	70	80	91	161	70	130	70	150	80
2/03	8		1		0	60	170	70	190	80	140	71	151	90	160	70	200	70	551	80	220	80	251	70	140	90	110	70	150	70	160	61	151	0
2/03	9	1			0	70	170	60	210	80	160	71	151	80	100	90	220	70	150	80	181	60	130	80	130	80	120	70	140	80	141	80	160	90
2/03	10		1		0	70	170	70	190	90	200	71	151	90	170	60	240	60	120	70	181	70	170	60	140	60	100	60	140	71	171	60	140	80
2/03	11			1	0	40	160	50	201	60	180	40	140	50	200	70	231	50	180	60	260	30	140	71	181	80	80	60	170	70	190	50	161	60
2/03	12			1	0	80	180	60	200	60	161	70	120	80	170	70	210	50	140	71	241	60	130	70	110	80	110	60	171	80	160	70	160	0
2/03	13	1			0	60	171	70	210	80	150	70	150	80	211	80	200	60	140	80	190	61	191	70	110	90	170	70	160	80	161	70	150	90
2/03	14		1		0	60	170	70	211	70	140	70	160	70	130	80	200	71	141	80	180	80	140	70	160	90	120	71	151	80	170	60	150	90
2/03	15		1		0	70	181	60	210	60	190	80	150	70	121	90	210	70	130	60	230	40	80	61	141	80	120	80	180	70	120	70	170	81
3/03	16		1		0	71	191	60	210	60	310	61	161	80	140	60	190	90	180	61	241	50	70	70	160	70	90	80	160	71	121	60	160	0
3/03	17	1			0	80	170	70	211	60	100	70	150	70	160	70	211	60	180	80	180	70	140	70	120	71	111	60	140	70	140	60	150	0
3/03	18		1		0	70	170	60	220	50	100	81	161	70	110	70	210	70	240	71	261	60	80	70	160	70	50	70	201	60	90	70	160	80
3/03	19			1	0	60	170	70	210	70	110	70	171	70	100	80	220	70	361	50	230	60	110	60	180	70	40	101	271	60	100	70	150	100
3/03	20			1	0	80	170	80	211	90	170	70	110	80	200	60	190	61	281	60	290	50	181	60	130	80	110	60	150	70	200	60	151	0
3/03	21		1		0	60	160	70	211	70	110	70	160	70	170	80	211	50	160	60	220	60	130	60	120	81	101	50	170	60	130	70	150	0
3/03	22			1	0	60	160	70	220	70	200	60	161	70	160	70	220	60	180	60	221	60	120	70	160	90	100	70	180	91	171	60	150	80
3/03	23		1		0	61	151	70	200	70	130	70	160	70	121	80	190	60	90	90	190	70	140	81	101	90	140	70	150	70	160	70	150	0
3/03	24			1	0	10	10	20	180	60	171	70	140	70	130	90	210	80	131	70	230	60	140	60	110	100	120	80	161	80	130	70	150	80
3/03	25		1		0	50	160	60	210	70	190	71	171	60	200	40	200	40	191	70	230	60	120	60	120	70	110	60	131	70	150	60	160	50

ANNEXE 16 - Signature biométrique de la frappe au clavier: population statistique utilisée (suite)

Population constituée de 155 échantillons d'une chaîne composée de 15 caractères. Ces échantillons ont chacun été prélevés à 10H30 (AM), 16H30 (PM) ou 22H30 (EV).
A chaque caractère correspond une durée d'intervale (IDT) et une durée de pression (DT).

Tableau A16.1 Population statistique utilisée (suite)

W#	Ech#	AM	PM	EV	K1		K2		K3		K4		K5		K6		K7		K8		K9		K10		K11		K12		K13		K14		K15	
					IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT
4/03	26	1			0	61	171	70	200	80	140	70	140	81	121	70	200	50	70	60	230	50	140	61	111	80	100	60	140	80	120	60	150	50
4/03	27		1		0	60	180	60	220	60	111	80	190	60	120	80	190	70	160	71	221	70	130	60	150	90	100	90	191	80	120	60	150	70
4/03	28	1			0	71	171	50	180	80	110	80	190	81	141	90	230	80	180	80	190	81	171	60	100	80	110	80	160	70	130	71	161	80
4/03	29		1		0	60	190	50	190	81	121	70	170	60	130	70	190	70	191	60	240	40	150	50	130	70	101	70	170	70	130	70	160	80
4/03	30	1			0	50	161	70	210	60	150	50	160	60	121	60	210	70	260	70	331	60	160	50	100	80	240	61	171	60	210	80	220	50
4/03	31	1			0	60	170	80	211	70	140	60	130	70	100	80	200	81	121	70	230	70	110	80	140	90	100	61	181	80	110	60	150	100
5/03	32	1			0	30	161	30	180	70	200	70	140	80	100	60	201	70	110	80	180	50	120	70	100	81	141	80	120	70	140	80	160	70
5/03	33		1		0	70	190	70	220	70	100	71	181	70	60	70	180	80	170	70	231	70	100	80	170	80	100	90	180	71	111	70	170	80
5/03	34	1			0	60	150	80	190	80	130	81	171	80	130	100	220	70	140	81	181	80	140	80	110	100	120	90	150	71	131	90	170	90
5/03	35		1		0	60	170	70	190	80	130	60	180	71	101	90	210	60	140	70	170	60	141	80	110	90	120	80	150	80	130	80	161	80
5/03	36	1			0	60	180	70	220	71	161	70	160	70	110	80	220	80	181	70	240	70	120	70	150	70	100	81	171	70	140	70	150	90
5/03	37		1		0	70	160	70	210	60	150	70	110	91	131	80	180	70	140	80	170	70	141	80	90	90	140	90	130	100	160	70	151	100
6/03	38	1			0	40	140	70	210	60	150	90	151	80	100	80	170	90	140	80	180	71	151	70	110	80	110	90	150	90	120	80	161	100
6/03	39		1		0	60	190	60	210	70	130	60	151	80	80	90	200	80	130	80	250	71	141	60	140	80	80	90	180	80	120	71	161	110
6/03	40	1			0	60	160	60	201	70	140	70	150	90	120	90	210	81	131	80	180	70	140	70	150	90	101	80	180	80	160	60	160	70
6/03	41		1		0	10	10	50	220	90	150	60	151	90	100	70	190	70	110	80	150	90	201	60	160	90	300	70	150	81	151	70	140	100
6/03	42	1			0	70	160	60	200	71	131	70	140	80	120	80	180	70	110	81	191	70	180	60	150	80	100	70	161	60	130	70	220	70
6/03	43		1		0	70	171	80	210	80	130	70	150	111	100	71	181	70	100	90	210	80	160	81	191	70	80	60	160	80	130	70	150	91
8/03	44	1			0	70	190	60	200	70	150	60	131	70	120	80	200	70	130	60	220	61	111	70	130	70	110	60	150	70	150	71	171	0
8/03	45		1		0	50	171	60	230	70	110	70	190	60	90	81	231	70	190	60	230	70	80	71	191	70	100	90	180	80	120	60	161	80
8/03	46	1			0	60	160	70	210	61	161	80	150	80	100	60	180	60	171	80	180	50	110	80	150	80	110	80	141	80	140	60	150	0
8/03	47		1		0	80	180	71	191	80	170	70	130	80	150	70	201	70	140	80	160	80	190	40	50	101	181	90	140	80	160	60	160	0
8/03	48	1			0	60	150	80	200	80	150	80	120	91	121	60	200	40	190	90	200	71	171	70	110	90	120	70	160	80	181	60	130	90
9/03	49	1			0	70	180	70	201	80	130	70	140	80	100	90	210	60	191	90	200	70	140	90	110	90	120	71	121	80	140	70	150	90
9/03	50		1		0	60	180	50	191	60	110	60	160	60	80	50	170	70	121	60	200	60	100	70	130	60	90	70	131	70	120	80	160	0

ANNEXE 16 - Signature biométrique de la frappe au clavier: population statistique utilisée (suite)

Population constituée de 155 échantillons d'une chaîne composée de 15 caractères. Ces échantillons ont chacun été prélevés à 10H30 (AM), 16H30 (PM) ou 22H30 (EV).
A chaque caractère correspond une durée d'intervale (IDT) et une durée de pression (DT).

Tableau A16.1 Population statistique utilisée (suite)

W#	Ech#	AM	PM	EV	K1		K2		K3		K4		K5		K6		K7		K8		K9		K10		K11		K12		K13		K14		K15	
					IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT
9/03	51		1		0	60	170	71	211	60	90	70	150	60	60	50	170	60	131	60	210	60	80	60	160	70	100	70	141	60	120	60	150	70
9/03	52	1			0	70	170	60	170	80	120	70	141	70	90	70	170	70	110	80	180	70	141	70	100	90	130	60	140	80	140	80	161	0
10/03	53	1			0	80	170	81	211	60	70	80	180	90	160	80	201	90	100	80	170	70	130	70	100	90	121	70	120	80	160	80	160	0
10/03	54		1		0	60	160	80	211	60	110	60	150	80	60	70	190	60	80	81	161	70	140	70	100	90	130	60	110	90	161	60	150	0
10/03	55			1	0	60	170	70	200	70	120	60	131	80	100	50	170	60	100	80	210	70	101	70	120	100	110	60	160	80	120	60	130	0
11/03	56	1			0	80	170	60	180	81	131	70	120	80	120	50	160	70	140	71	171	70	110	70	120	80	110	60	150	70	151	50	140	80
11/03	57		1		0	60	170	60	190	80	140	70	131	80	110	80	210	60	120	70	241	60	110	70	130	80	100	50	150	70	140	71	151	90
11/03	58			1	0	70	170	61	211	80	120	60	150	80	90	70	191	70	110	70	230	60	110	70	150	71	91	90	160	80	140	70	160	0
11/03	59		1		0	60	160	70	221	60	110	50	150	70	70	60	180	30	110	61	211	70	130	60	100	90	100	70	150	81	101	70	160	70
11/03	60			1	0	70	190	60	200	70	160	60	131	80	90	70	190	70	150	60	230	61	131	50	150	70	60	80	190	80	100	60	161	80
11/03	61			1	0	60	171	70	200	80	150	80	150	70	141	50	180	80	130	80	210	70	171	70	100	90	140	90	160	90	160	70	161	80
11/03	62	1			0	70	181	50	170	70	160	60	130	80	130	91	231	60	120	70	170	70	120	60	121	80	80	60	170	70	110	70	170	60
11/03	63		1		0	50	150	81	211	70	140	70	150	80	230	91	231	70	160	90	160	90	150	81	101	100	140	80	150	90	140	60	160	81
11/03	64	1			0	50	170	50	211	70	130	70	170	60	70	90	200	80	121	60	200	70	120	70	140	80	90	80	151	80	120	70	160	0
11/03	65	1			0	81	171	60	190	80	250	80	171	80	180	60	170	80	160	90	191	80	170	70	180	90	401	70	150	70	200	60	150	81
11/03	66		1		0	60	171	60	220	70	300	70	161	70	150	110	210	60	90	80	190	61	131	70	100	100	120	80	150	90	190	61	151	90
11/03	67			1	0	40	150	70	210	80	150	80	151	80	80	80	170	90	140	80	230	81	121	90	180	80	40	100	210	80	100	60	151	90
12/03	68		1		0	60	180	50	201	60	90	70	180	60	80	80	240	61	121	60	240	60	200	70	130	71	101	80	160	70	120	70	160	0
12/03	69	1			0	60	181	60	200	70	110	90	160	70	100	61	181	70	130	60	210	70	120	60	121	80	90	70	170	80	120	60	150	80
12/03	70		1		0	70	170	71	191	90	120	70	170	90	110	70	181	80	160	70	160	70	120	70	110	91	121	70	130	80	150	60	150	80
12/03	71			1	0	90	191	60	210	80	130	70	170	90	70	91	191	80	140	80	200	80	150	81	121	100	140	100	180	100	160	80	171	100
12/03	72			1	0	60	180	71	201	80	160	60	160	70	80	70	201	70	110	70	230	60	110	90	160	71	91	80	170	70	100	70	160	80
12/03	73	1			0	40	150	70	200	70	120	71	161	80	60	60	190	60	110	70	180	61	101	70	140	80	110	80	160	70	130	70	151	60
12/03	74		1		0	60	170	70	221	70	140	60	170	70	30	90	251	60	160	70	220	60	120	60	150	81	81	80	180	70	120	60	150	0
12/03	75		1		0	50	150	70	220	60	141	50	170	70	60	80	210	50	150	70	171	60	120	70	110	100	150	70	150	101	161	70	170	80

ANNEXE 16 - Signature biométrique de la frappe au clavier: population statistique utilisée (suite)

Population constituée de 155 échantillons d'une chaîne composée de 15 caractères. Ces échantillons ont chacun été prélevés à 10H30 (AM), 16H30 (PM) ou 22H30 (EV).
A chaque caractère correspond une durée d'intervale (IDT) et une durée de pression (DT).

Tableau A16.1 Population statistique utilisée (suite)

W#	Ech#	AM	PM	EV	K1		K2		K3		K4		K5		K6		K7		K8		K9		K10		K11		K12		K13		K14		K15	
					IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT
13/03	76	1			0	60	170	60	200	70	100	70	171	80	70	60	190	40	100	80	170	90	120	71	151	80	100	90	180	80	120	60	150	81
13/03	77		1		0	50	160	60	191	70	170	60	160	80	100	60	190	61	121	70	160	80	130	80	150	80	120	91	141	80	150	80	170	0
13/03	78			1	0	70	180	80	220	70	131	70	180	80	90	90	200	60	100	80	171	80	110	80	160	90	100	90	180	90	121	60	160	80
13/03	79	1			0	40	160	60	210	70	120	70	160	71	111	80	210	60	170	60	210	71	111	70	160	70	100	70	170	70	130	81	161	80
13/03	80		1		0	60	161	60	190	70	120	70	160	80	120	81	201	80	170	70	160	70	140	80	100	81	121	70	160	70	110	70	160	0
13/03	81			1	0	70	190	60	220	70	170	71	141	70	110	80	190	70	150	60	231	60	130	50	130	90	100	60	210	81	131	60	160	70
13/03	82			1	0	70	180	71	231	60	100	70	170	70	90	60	181	70	170	50	210	60	110	60	160	81	101	80	180	70	140	70	150	90
13/03	83	1			0	50	160	50	190	80	160	71	151	90	110	50	160	80	120	80	170	71	111	70	130	80	120	60	150	70	140	71	171	80
13/03	84		1		0	70	190	80	240	81	111	80	180	80	140	60	210	60	90	91	191	80	150	80	140	100	130	70	191	100	170	70	170	100
13/03	85			1	0	60	180	70	230	80	190	61	141	80	110	70	180	60	130	80	191	90	130	70	150	90	120	60	160	91	161	60	160	80
13/03	86	1			0	41	151	60	210	60	200	60	141	100	110	70	210	70	120	60	220	71	131	70	140	90	80	70	160	70	130	70	151	80
13/03	87			1	0	60	170	70	200	80	180	70	171	80	80	80	180	70	110	70	220	71	141	70	130	80	70	90	180	80	160	71	161	80
14/03	88	1			0	60	160	60	190	60	160	81	131	70	120	110	220	90	180	70	261	60	170	70	140	80	100	80	171	70	140	70	170	80
14/03	89		1		0	60	180	70	210	80	431	90	220	90	140	81	201	60	140	80	170	70	120	70	121	90	120	90	160	90	140	90	170	111
14/03	90			1	0	60	181	70	230	80	210	70	161	90	90	70	210	80	160	80	231	70	130	80	160	90	100	70	180	70	151	70	170	90
14/03	91	1			0	50	170	60	221	60	140	80	180	70	60	90	200	71	131	70	240	60	130	80	150	91	81	100	200	70	120	60	150	90
14/03	92		1		0	60	180	70	221	70	130	80	180	70	50	60	200	61	191	70	220	80	170	70	140	81	111	70	170	80	120	70	170	70
14/03	93			1	0	40	170	50	230	60	171	60	160	70	90	70	200	60	140	61	221	50	120	70	160	100	60	70	241	60	130	60	150	70
14/03	94			1	0	70	190	70	221	70	210	80	170	80	120	101	221	70	200	80	230	70	151	50	120	80	100	90	190	70	130	60	151	0
14/03	95			1	0	60	170	70	220	90	201	80	190	80	90	60	200	70	141	80	240	60	150	70	120	80	100	91	201	70	150	60	160	80
14/03	96	1			0	60	171	70	210	70	190	70	140	70	110	71	211	60	110	60	210	60	150	61	131	80	100	50	180	60	140	70	171	80
14/03	97	1			0	60	160	80	251	80	200	70	200	70	110	70	221	60	170	70	210	60	120	71	131	100	90	80	190	70	150	60	140	81
14/03	98		1		0	60	170	70	190	70	120	60	150	81	60	71	181	80	140	60	190	60	140	61	111	90	90	90	180	80	120	60	140	80
14/03	99	1			0	81	181	60	190	70	190	70	160	91	111	90	190	90	120	70	140	70	130	81	101	90	140	100	120	70	170	80	160	111
14/03	100		1		0	60	171	70	220	70	160	60	150	80	121	70	180	80	140	80	180	70	120	71	151	90	120	70	170	80	170	70	171	90

ANNEXE 16 - Signature biométrique de la frappe au clavier: population statistique utilisée (suite)

Population constituée de 155 échantillons d'une chaîne composée de 15 caractères. Ces échantillons ont chacun été prélevés à 10H30 (AM), 16H30 (PM) ou 22H30 (EV).
A chaque caractère correspond une durée d'intervale (IDT) et une durée de pression (DT).

Tableau A16.1 Population statistique utilisée (suite)

W#	Ech#	AM	PM	EV	K1		K2		K3		K4		K5		K6		K7		K8		K9		K10		K11		K12		K13		K14		K15	
					IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT
14/03	101			1	0	50	160	71	211	80	100	80	170	80	100	80	211	60	80	80	170	80	120	90	130	90	120	71	161	60	150	60	170	0
15/03	102	1			0	70	180	60	200	80	190	71	171	90	120	70	190	50	140	80	171	80	150	70	120	90	110	90	170	90	151	70	180	70
15/03	103		1		0	50	170	70	221	70	140	70	160	60	90	80	200	71	171	70	220	70	120	70	150	70	100	111	171	70	150	70	160	110
15/03	104			1	0	50	150	90	241	70	160	80	220	70	160	80	221	60	180	50	210	70	120	60	201	80	100	100	210	70	130	70	161	100
15/03	105	1			0	50	180	51	201	60	120	50	170	70	130	60	181	60	110	60	210	50	90	60	150	81	81	70	180	70	140	50	140	70
15/03	106		1		0	71	171	90	220	80	130	70	150	91	111	60	180	70	110	80	180	60	120	71	151	100	120	70	190	90	160	70	161	90
15/03	107			1	0	50	180	60	201	70	130	80	170	90	90	70	241	50	80	90	200	70	130	90	110	100	161	90	120	90	170	70	160	0
15/03	108			1	0	60	170	70	210	90	200	50	161	90	70	70	210	50	140	70	241	60	200	70	120	100	130	80	170	91	211	30	130	0
15/03	109		1		0	70	181	70	220	80	130	100	200	90	141	90	230	80	120	70	190	70	171	60	130	80	110	90	190	80	130	70	161	90
15/03	110			1	0	80	210	80	200	80	191	70	170	80	120	70	210	60	191	80	210	90	210	60	180	91	131	90	180	80	220	60	150	91
15/03	111	1			0	70	170	60	201	70	150	70	170	70	50	70	230	71	171	80	200	70	130	70	140	90	111	90	160	80	150	70	140	100
15/03	112		1		0	40	161	70	250	70	130	70	190	80	90	81	211	50	90	90	170	80	130	70	151	90	120	70	170	90	140	70	180	71
15/03	113			1	0	70	190	70	220	80	211	80	190	70	80	90	210	90	221	80	190	70	180	70	100	90	181	110	190	80	200	80	170	0
15/03	114	1			0	60	170	80	230	70	120	70	161	70	130	60	170	70	140	70	231	60	120	60	150	80	100	60	170	70	151	70	170	80
15/03	115		1		0	70	170	50	200	71	141	60	170	70	180	110	251	90	100	80	190	70	100	80	160	90	121	100	160	80	140	70	160	90
15/03	116			1	0	70	181	80	230	70	180	60	140	91	111	70	200	70	80	80	170	60	100	80	141	90	130	80	140	90	180	70	160	0
15/03	117	1			0	70	170	60	210	70	140	81	191	90	60	80	210	60	110	80	171	80	80	90	180	90	120	80	160	80	100	71	161	100
15/03	118		1		0	70	170	50	181	80	130	70	150	90	60	80	170	80	140	81	151	80	90	80	180	80	80	100	180	101	141	90	160	100
15/03	119			1	0	91	161	80	240	70	280	60	151	70	150	100	230	90	130	70	231	80	130	70	160	60	70	90	150	81	161	70	160	100
16/03	120	1			0	51	161	70	200	80	150	70	150	81	191	80	240	80	100	80	160	81	141	90	120	90	140	100	120	90	170	81	171	80
16/03	121			1	0	90	200	80	190	100	140	111	201	100	230	100	260	81	411	90	220	70	171	80	110	80	120	100	160	90	170	91	171	0
16/03	122	1			0	50	181	60	200	70	200	60	130	70	110	81	201	70	120	70	230	60	120	81	151	80	100	90	170	80	150	60	160	91
16/03	123			1	0	60	170	81	251	60	130	70	130	60	120	70	191	70	120	70	220	60	100	80	150	91	111	70	160	100	190	70	160	81
16/03	124			1	0	81	201	80	240	80	140	80	160	101	131	70	180	70	100	90	180	80	100	81	151	110	150	70	170	100	190	81	181	90
16/03	125		1		0	60	170	70	221	60	200	60	160	90	100	80	201	60	110	80	180	80	120	90	140	101	121	90	170	80	130	80	180	100

ANNEXE 16 - Signature biométrique de la frappe au clavier: population statistique utilisée (suite)

Population constituée de 155 échantillons d'une chaîne composée de 15 caractères. Ces échantillons ont chacun été prélevés à 10H30 (AM), 16H30 (PM) ou 22H30 (EV).
A chaque caractère correspond une durée d'intervale (IDT) et une durée de pression (DT).

Tableau A16.1 Population statistique utilisée (suite)

W#	Ech#	AM	PM	EV	K1		K2		K3		K4		K5		K6		K7		K8		K9		K10		K11		K12		K13		K14		K15	
					IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT
16/03	126	1			0	50	160	71	211	70	120	70	170	70	80	50	171	50	80	80	170	80	120	60	140	100	90	101	181	80	140	60	150	0
16/03	127		1		0	61	171	60	230	60	130	60	160	71	101	60	170	70	100	60	230	60	111	90	140	70	100	100	160	60	140	60	150	0
16/03	128			1	0	40	160	60	220	70	140	80	181	80	50	80	200	80	130	60	231	70	120	80	160	80	100	120	180	80	151	70	160	0
16/03	129		1		0	90	200	70	220	80	110	70	171	90	120	80	220	60	140	70	141	80	90	70	160	90	110	70	170	90	160	71	181	80
16/03	130			1	0	20	130	50	190	80	160	71	161	90	100	80	190	70	90	80	160	81	141	80	110	100	140	100	170	90	160	51	171	90
16/03	131		1		0	50	170	70	231	80	140	70	170	90	150	70	221	60	90	100	170	90	130	70	140	110	110	71	161	90	160	60	150	80
16/03	132			1	0	70	190	71	221	80	140	70	210	70	120	91	241	70	110	60	230	60	110	70	141	70	100	110	160	80	170	60	150	0
17/03	133	1			0	60	180	60	210	70	151	70	180	70	20	80	250	60	120	80	171	70	50	60	190	90	100	110	170	80	141	70	170	0
17/03	134		1		0	50	161	70	200	70	150	60	180	80	181	50	170	80	80	80	170	80	110	91	131	90	140	100	130	100	210	80	160	0
17/03	135			1	0	60	171	70	200	80	170	60	160	81	91	70	210	50	100	90	190	70	30	80	241	80	150	60	120	80	200	70	171	60
17/03	136	1			0	70	180	80	210	81	141	70	150	80	140	90	200	70	121	70	240	60	90	70	190	80	50	111	241	70	140	90	160	120
17/03	137		1		0	70	170	70	210	81	131	90	170	80	120	80	200	80	90	81	221	90	150	80	130	110	100	80	181	120	150	90	190	80
17/03	138			1	0	51	191	60	220	70	190	70	131	80	120	60	170	60	110	70	160	90	151	70	110	90	150	80	150	90	170	60	161	0
17/03	139		1		0	70	170	80	220	70	130	80	161	100	100	80	180	90	90	80	170	80	110	91	121	110	130	100	140	100	170	70	160	0
17/03	140			1	0	50	170	50	190	70	140	70	191	60	70	80	190	70	100	60	230	60	161	90	130	80	130	100	150	90	150	71	151	0
17/03	141	1			0	50	161	60	190	60	190	70	150	100	110	61	181	70	120	70	210	70	140	70	161	80	100	60	180	80	140	70	160	0
17/03	142		1		0	60	180	70	200	80	120	70	151	90	180	70	230	60	40	90	190	71	151	80	100	90	140	80	150	110	181	60	150	90
17/03	143			1	0	70	170	80	220	90	200	81	171	90	120	70	210	70	100	90	181	90	170	80	120	100	170	30	140	101	201	50	140	80
17/03	144	1			0	50	160	70	190	90	170	70	151	80	90	70	180	70	100	80	160	80	80	81	171	110	90	80	190	90	140	70	161	90
17/03	145		1		0	80	191	60	200	70	110	70	170	90	90	51	171	80	140	50	240	60	100	71	161	80	110	60	170	70	140	80	170	0
17/03	146			1	0	70	190	70	210	70	100	70	170	91	101	50	150	60	170	70	220	71	181	60	110	80	120	60	170	70	170	71	161	80
18/03	147	1			0	20	131	80	220	80	180	80	160	91	241	40	190	70	190	70	191	70	140	70	130	100	150	90	160	101	221	60	170	90
18/03	148		1		0	40	160	80	210	60	180	80	161	60	130	70	200	70	100	70	170	81	141	70	120	90	140	90	140	80	160	61	161	110
18/03	149	1			0	50	170	60	210	70	131	80	170	90	140	60	180	70	80	80	171	80	120	80	150	110	130	70	170	91	151	70	170	90
18/03	150	1			0	50	170	50	190	70	120	60	161	70	100	70	190	60	110	60	230	61	81	90	170	60	110	80	180	80	150	61	161	90

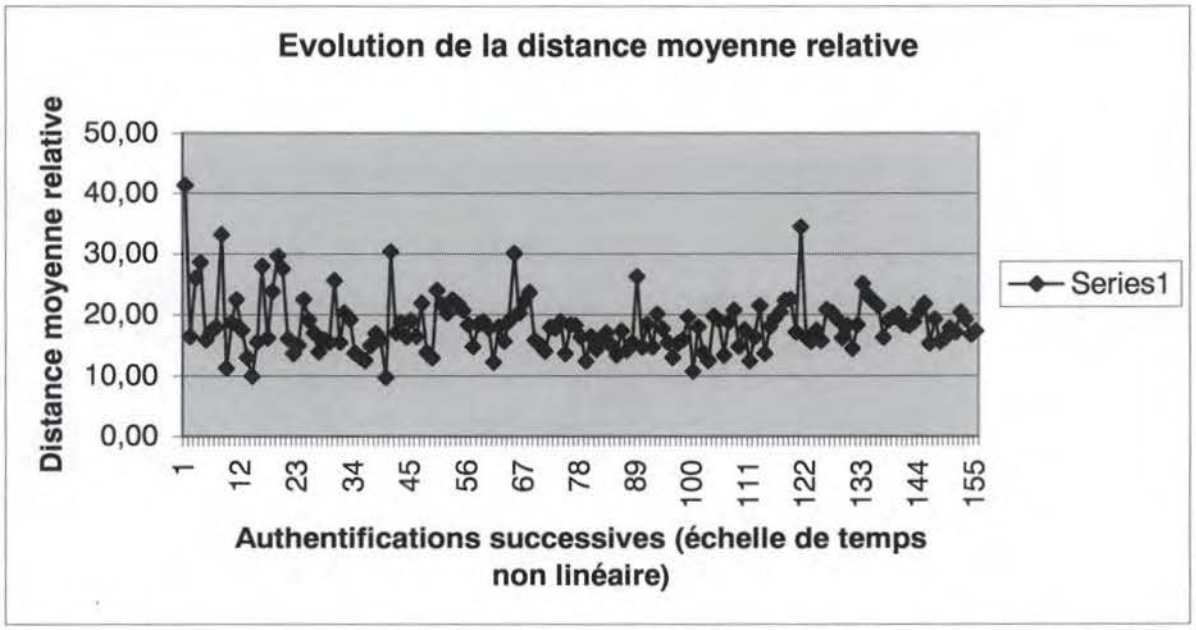
ANNEXE 16 - Signature biométrique de la frappe au clavier: population statistique utilisée (suite)

Population constituée de 155 échantillons d'une chaîne composée de 15 caractères. Ces échantillons ont chacun été prélevés à 10H30 (AM), 16H30 (PM) ou 22H30 (EV).
A chaque caractère correspond une durée d'intervale (IDT) et une durée de pression (DT).

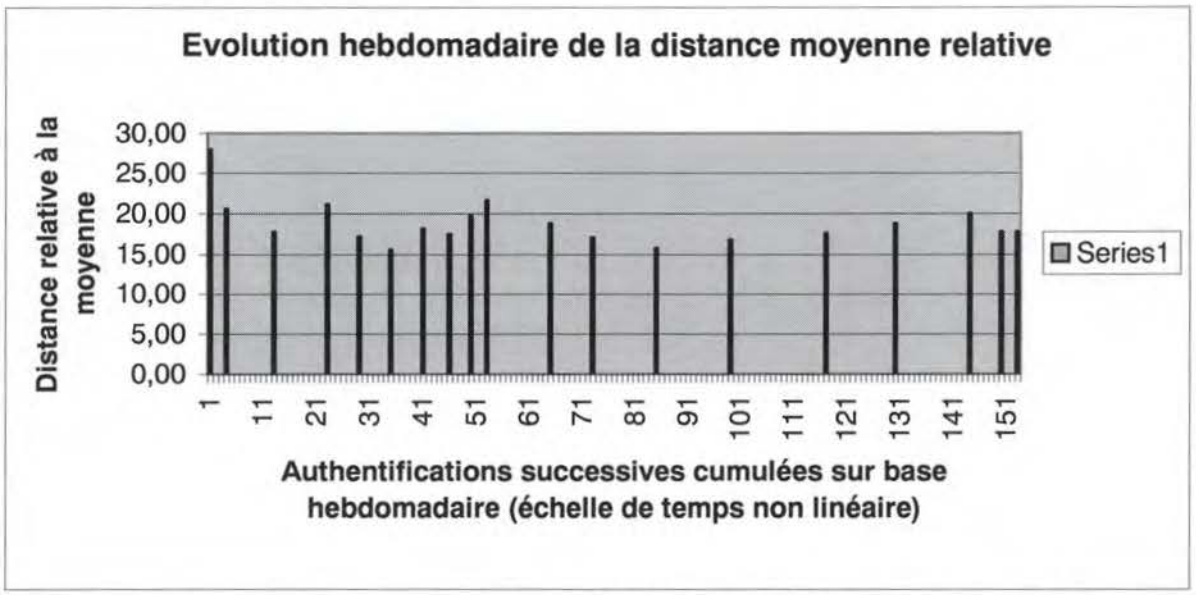
Tableau A16.1 Population statistique utilisée (suite)

W#	Ech#	AM	PM	EV	K1		K2		K3		K4		K5		K6		K7		K8		K9		K10		K11		K12		K13		K14		K15	
					IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT	IDT	DT
18/03	151	1			0	50	161	70	190	80	190	80	180	80	111	90	200	80	120	60	220	70	130	71	131	80	110	90	160	80	140	80	160	0
18/03	152	1			0	20	150	50	210	61	111	80	180	70	90	60	190	70	110	71	231	60	140	70	90	80	140	100	130	91	191	80	190	70
19/03	153	1			0	50	160	60	220	60	150	81	181	90	170	100	220	80	130	71	151	80	120	90	130	100	130	110	150	91	181	70	160	0
19/03	154	1			0	50	171	50	190	60	110	70	140	80	100	60	171	60	130	70	170	60	140	70	100	90	130	71	131	90	160	80	160	80
19/03	155	1			0	50	150	60	210	71	111	70	180	70	90	70	190	80	90	61	201	70	120	70	130	80	110	70	140	81	131	70	150	90

ANNEXE 17 - Signature biométrique de la frappe au clavier : Evolution dans le temps de la distance relative



Graphe A17.1: évolution (en continu) de la distance relative



Graphe A17.2: évolution de la distance relative sur base hebdomadaire

ANNEXE 18 - Page du manuel de RAT

SunOS 5.5.1 Last change: 22 February 1997

NAME
rat - unicast and multicast audio conferencing tool

SYNOPSIS
rat [options] addr/port
rat -F [options] infile outfile
rat -T [options] addr/port/ttl/codec addr/port/ttl/codec

OPTIONS
The following options are supported:

-crypt key
Enable encryption, with the specified key. Encryption is done using DES, and is believed compatible with encrypting versions of vat.

-drop drop
Specifies the percentage of packets to be dropped at the transmitter. This is particularly useful when experimenting on files for testing how a given repair/coding technique works.

-f c1/c2/../cn
Specifies the encodings used when transmitting audio. The order is primary encoding, secondary ncoding, etc. A maximum of seven levels of encoding are possible, although only two are available from the user interface. The allowed values are l16, pcm, dvi, gsm, lpc. See CODECS below for description of the codecs and their recommended usage.

-F infile outfile
Makes RAT to read audio from the file infile , encode it, and transmit it on the local loopback address, and inally write it to outfile. This is useful inconjunction with the -drop option for evaluating repair techniques and codecs. The file format is 16 bit linear PCM audio, currently sampled at 8 kHz, with no header nformation.

-loopback_rtp
Causes rtp packets to be loopbacked during multicast sessions.

-lbl_channel channel
Specifies the channel identifier for use with the LBL Conference Bus. RAT always listens to the base channel for audio device trading with other tools, like vat(1). When a channel is specified it allows RAT to communicate with other tools, like vic(1), provided they have the same channel number. This is particularly useful for voice switching the video sources.

-lbl_priority priority
Specifies the processing priority of the code that handles the LBL Conference Bus. The default value is 100 and the permitted range of values is 0 to 200.

-name name
Sets the RAT window title to name.

-no_ui
Do not display user interface.

ANNEXE 18 - Page manuel de RAT (suite)

-p priority
Sets the thread priority on the Windows 32-bit version. The following values are observed:
1 above normal priority level
2 time critical thread priority
3 highest thread priority

-pt type/redundancy
Specifies the dynamic payload type to be used for redundancy. Later versions will accept configurable payload types for the primary encoding.

-repair method
Specifies the use of receiver based repair technique based on method. This can currently be none or repeat.

-t ttl
Specifies the TTL (time to live) value set in the packet headers. This limits the scope of the packets. The following values are generally considered appropriate:
4 campus/organization
16 country
64 continent
127 planet

-T addr/port/ttl/codec addr/port/ttl/codec
Causes RAT to operate as an RTP transcoder/mixer. In this mode the user-interface is not displayed, and no audio is played out. Instead, RTP packets received from either group are transcoded into the ormat specified for the other group, multiple sources are mixed together, and the result transmitted to the other group. In each case, addr may be either unicast or multicast, and the ttl and codec specifiers may be omitted (The default is TTL 16, DVI coding). This option is useful for transcoding between low- and high-bandwidth sessions, for use other a slow link, for example.

-seed number
Seeds the random number generator that governs dropping of packets at the transmitter. Only valid in conjunction with the -drop option.

-silence on|off
Turns silence suppression on or off. hysteresis. If the packet average is greater than the threshold for interval packets, the minimum average value is incremented by one, but not beyond max_avg.

-version
Displays the version number.

DESCRIPTION
RAT is a network audio tool that allows users to particpate in conferences over the internet. These can be between two participants directly (unicast) or between a group of participants on a common multicast address. To initiate a unicast conference the user specifies the destination host name or IP address and a port number. To participate in a multicast conference a Class D group address should be specified together with a port number. The application uses the greatest even integer less than or equal to the port specified for data (RTP) and the port above for control messages (RTCP). The protocols RTP and RTCP used are specified in RFC 1889.

ANNEXE 18 - Page manuel de RAT (suite)

USER INTERFACE

Main Window

The main window of RAT is split into three sections. On the left is a list of conference participants, below this are a number of buttons enabling setting of options, and on the right are volume/microphone controls. The list of participants shows local and remote conference members. Active speakers are highlighted. Clicking the left mouse button on the name of a remote participant will display a user information panel, giving various reception statistics for that user. Individuals can be selectively muted by clicking on them with the middle mouse button on three button systems, or moving the mouse to the individual and pressing the m. The right-hand side of the RAT window contains volume and gain controls. The leftmost controls in this section control audio output, and the rightmost control audio input. The sliders control volume/gain, and the icons above them select audio source and destination. Audio output may be toggled between speaker, headset and line out. Audio input may be toggled between microphone and line in. Audio input/output may be independently muted. Pressing the right mouse button anywhere within the RAT window will temporarily toggle the state of the audio input mute: this allows a "push-to-talk" mode of operation.

Options

Pressing the "options" button brings up a control panel, allowing the operation of RAT to be modified. The options in this panel are as follows:

Duration

Select amount of audio data, in milliseconds, which is sent in each packet. Larger values result in greater end-to-end delay over the network, but reduce the perpacket header overhead.

Encodings

Sets the format for data transmitted to the network. If the conference includes vat users, redundancy should be turned off; however if all users are using RAT, and packet loss is being experienced, the use of redundancy will vastly improve sound quality. It is hoped that future versions of vat will eventually be able to decode redundant audio data.

Mode

Determines whether audio data from the network has priority over outgoing data. Use options other than full duplex with caution, since they can be confusing.

Loss repair

If set to packet repetition the receiver attempts to patch over missing packets with the replay of the previous packet. This is a receiver based solution to the problem of network packet loss. We recommend that redundancy is used in these cases, but if that is not possible, use of this option may help. This does not affect the data sent to the network.

Suppress Silence

If on periods of silence within a conversation are not transmitted, reducing the network traffic. We recommend that this option is on.

Powermeters

If on, audio powermeters will be displayed in the main RAT window.

Lecture Mode

If on, the playout delay at the receiver is artificially increased. This results in better performance in the presence of variable network delay, at the expense of reduced interactivity. It is most useful when listening to broadcast lectures, hence the name. This is automatically turned off if you transmit audio.

ANNEXE 18 - Page manuel de RAT (suite)

Video Synchronisation
If using a modified version of vic, this enables lip synchronisation between audio and video streams. This is not generally useful at present.

Automatic Gain Control
If on, the microphone gain will be controlled automatically.

Acoustic Feedback
If on, acoustic feedback of input gain will be provided.

Play file/Rec file
Allow the playback/recording of audio data in the conference. Format of the files is raw 8kHz 16bit linear PCM data, with no headers.

RTP info
Allows setting of the name by which you appear in the conference.

Session key
Entering a key, and enabling this will encrypt the audio data using DES. This encryption is believed compatible with encrypting versions of vat.

CODECS

Five types of audio encoding are currently possible with RAT, although more are in development. The encodings are:

Name	Bit rate	Description
l16	128 kb/s	Linear PCM at 16 bits per sample.
pcm	64 kb/s	Mulaw companded PCM at 8 bits per sample (G711).
dvi	32 kb/s	Intel's DVI ADPCM at 4 bits per sample.
gsm	13.2 kb/s	EDSI Group Systeme Mobile codec.
lpc	5.8 kb/s	Ron Zuckerman's 10 pole LPC codec.

Internally, RAT uses 16 bit linear sampling at 8 kHz (except on hardware where it is unavailable, then 8 bit mulaw is used). Multiple sampling rates will be available in a future release.
NB The DVI codec has 4 bytes of state associated with each packet irrespective of it's length.

PACKET OVERHEADS

There is an overhead associated with each audio packet sent. When RAT is operating as an audio tool the RTP header is 96 bits per packet (it is longer when RAT is acting as mixer and there are multiple contributing sources in each packet. The UDP/IP overhead is 224 bits per packet. Thus transmitting with 20 ms packets has an overhead of 11.2 kb/s, whereas 80 ms only incurr 2.8 kb/s. By default RAT starts with 40 ms packets of DVI coded data. This represents a trade off between bandwidth, quality, and the ability of receiver based repair techniques to work successfully.

EXAMPLES

To start a unicast session between the current host and the host shrew.cs.ucl.ac.uk using port 12000 type:

```
rat shrew.cs.ucl.ac.uk/12000
```

To join a multicast session on group address 224.5.6.7 and port 8110 type, using primary encoding of dvi and a secondary encoding of lpc:

```
rat -f dvi/lpc 224.5.6.7/8110
```

ANNEXE 18 - Page manuel de RAT (suite)

To simulate packet loss between 2 hosts of 10% using trek.in as the input file and trek.out as output file:

rat -F -drop 10 trek.in trek.out

AUTHORS

The original RAT code was developed by Vicky Hardman <V.Hardman@cs.ucl.ac.uk> and Isidor Kouvelas <I.Kouvelas@cs.ucl.ac.uk> at University College London. The DES encryption was written by Saleem Bhatti <S.Bhatti@cs.ucl.ac.uk> and integrated by Darren Harris. This release of RAT has been substantially enhanced by Isidor Kouvelas, Colin Perkins <C.Perkins@cs.ucl.ac.uk>, and Orion Hodson <O.Hodson@cs.ucl.ac.uk>. The RAT project is managed by Vicky Hardman and Angela Sasse, and supported by the following projects:

MICE Multimedia Conferencing in Europe (ESPRIT)
MERCI Multimedia European Research Conferencing Integration
ReLaTe Remote Language Teaching for Super Janet (BT/JISC)
RAT Robust Audio Tool (EPSRC/BT)

ACKNOWLEDGEMENTS

We thank Anna Watson, Mark Handley, Steve Casner, Jon Crowcroft, Atanu Ghosh, Roy Bennett, Jane Hughes, Marcus Iken, and our collegues at UCL who have provided countless suggestions and extended good humour through the buggy prereleases. Modifications for HP-UX by Terje Vernly <terjeve@usit.uio.no> and Geir Harald Hansen <g.h.hansen@usit.uio.no>. This software is derived, in part, from publically available source code with the following copyright:

FEEDBACK

Please send comments and suggestions to rat-trap@cs.ucl.ac.uk.
Please check ftp://www.cs.ucl.ac.uk/mice/rat for latest release information.

ANNEXE 19 - Les critères communs

A19.1. Introduction

A19.1.1. Avertissement

Approcher les Critères Communs (CC) sur un seul chapitre relève de la gageure, chacun des documents produits dans le cadre de l'application rigoureuse de cette outil pouvant pratiquement, à lui seul, faire l'objet d'un travail de fin d'études. Notre objectif ici n'est donc pas d'en décrire de manière détaillée les principes, avantages et limites éventuelles, et l'ambition de ce chapitre n'est pas d'en constituer un didacticiel; les pages qui suivent ne constituent donc pas une vue complète de la méthode, mais une illustration de ce qu'elle peut produire.

A19.1.2. Finalité

Les Critères Communs (Common Criteria, ou CC) sont avant tout une méthode de normalisation de l'expression des exigences de sécurité dont l'objectif essentiel est l'établissement de la confiance dans la sécurité des TI, confiance basée sur l'utilisation parallèle d'exigences d'assurance - tant sur le produit que sur son développement - et d'une échelle d'évaluation.

A19.1.3. Contexte

Les CC sont le résultats d'efforts multilatéraux pour développer, regrouper et normaliser des critères utilisés dans le cadre de l'évaluation de la sécurité des TI. La plus ancienne contribution à l'origine des CC remonte au début des années 1980 avec la publication aux Etats-Unis des TCSEC (*orange book*[107]) [TCSEC], alors qu'en Europe c'est à l'instigation de la Commission Européenne au début des années 1990 qu'un premier effort de normalisation des critères français, allemands et anglais (*UK Confidence Levels*) menait à la publication de la norme ITSEC 1.2 (1991) [ITSEC]

La mise en place début des années 1990 à l'ISO d'une commission d'experts (ISO/IETC JTC1 / SC27 / WG3), la publication au Canada de la norme CTCPEC 3.0 (1993) [CTCPEC], inspirée des TCSEC et influencée par l'ITSEC, et celle aux Etats-Unis du draft des FC 1.0 (Federal Criteria, 1993) [FC] marquèrent le début de la convergence pan-Atlantique. Dans le but de contribuer à l'effort de l'ISO, les différentes organisations commanditaires des normes précitées (TCSEC, ITSEC, CTCPEC et FC) lancèrent en commun le projet CC. Le résultat de ces efforts combinés sont les CC version 2.0 (1998) lesquels, après quelques modifications mineures, devinrent la norme officielle ISO/IEC 15408 aussi appelée CC 2.1 (1999) et intitulée *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information.*

A19.1.4. Audience

Les CC contiennent des informations et méthodes à l'usage des utilisateurs, développeurs, et évaluateurs de produits ou systèmes aussi appelés TOE (Target Of Evaluation).

Aux utilisateurs, elle fournit des références et informations générales pour formuler leurs exigences dans le domaine de la sécurité et déterminer le niveau d'assurance requis. Les développeurs y trouveront matière pour le développement des exigences, la formulation des spécifications de sécurité, ainsi que la compréhension des exigences fonctionnelles et d'assurance. Les évaluateurs s'en serviront pour déterminer les critères d'évaluation obligatoires en vue d'assurer que la TOE réalise effectivement les fonctions de sécurité requises.

[107] http://www.dynamoo.com/orange/summary.htm

ANNEXE 19 - Les critères communs (suite)

A19.1.5. Matériel

Les critères communs sont constitués en trois parties. La première partie, *Introduction et modèle général* [CC-1], en définit les concepts généraux alors que les deuxième et troisième parties en constitue le catalogue des exigences fonctionnelles (Partie 2: *Exigences de sécurité fonctionnelles*) [CC-2] et d'assurance (Partie 3: *Exigences de sécurité d'assurance*) [CC-3]. Notons pour information que certaines documentions complémentaires existent, tels des guides pour conduire des évaluations ou construire certains documents.

Pour cette étude, nous nous sommes basés uniquement sur les parties 1 à 3 des CC 2.0. Le choix de la cette version (2.0 au lieu de la version 2.1) n'est basé sur aucune autre motivation que celle de gagner du temps, la documentation de la version 2.0 étant la première que nous ayons trouvée en français sur un serveur canadien[108].

A19.2. Modèle général

A19.2.1. Introduction

Le principe de base des CC est que la confiance dans un système d'information peut être obtenue par le biais d'actions qui peuvent être entreprises au cours des phases de développement, d'évaluation et de production. Les CC définissent un ensemble d'exigences de sécurité et d'assurance, exigences dont la validité est connue, et qui peuvent être utilisées pour établir les exigences de sécurité des futurs produits et systèmes.

A19.2.2. Concepts de sécurité

Les CC envisagent la sécurité des TI selon une approche progressive que nous pourrions résumer comme suit:

- l'environnement de sécurité de la TOE
- les objectifs de sécurité de la TOE
- les exigences de sécurité de la TOE
- les spécifications de sécurité de la TOE
- l'implémentation de la TOE

L'environnement de sécurité de la TOE consiste en l'ensemble des lois, politiques de sécurité organisationnelles, coutumes, expertises, caractéristiques de l'environnement d'exploitation et menaces recensées (ou supposées). La définition de l'environnement de sécurité se base sur la connaissance de l'environnement physiques de la TOE, des objectifs de la TOE et de la nature des biens nécessitant protection; elle s'exprime par l'établissement d'un certain nombre d'hypothèses concernant le comportement de l'environnement de la TOE (ces hypothèses sont ensuite considérées comme des axiomes lors de l'évaluation de la TOE), d'une liste de menaces et d'un certain nombre de mesures de nature organisationnelle. C'est sur base de ces documents que peuvent ensuite être établis les objectifs de sécurité de la TOE.

La mise en relation de ces objectifs de sécurité avec le catalogue des exigences des CC permet d'établir les exigences de sécurité fonctionnelles de la TOE, les exigences sur l'environnement (technique et procédural) et les exigences d'assurance de la TOE. Pour terminer, les exigences sur la TOE (sécurité et assurance) sont converties en spécifications, c'est à dire que les exigences de sécurité sur la TOE sont instantiées sous la forme de définition de haut niveau des *fonctions de sécurité* (SF - *Security Functions*) et que les mesures d'assurances prises sont définies.

Une représentation schématique de ce qui précède, reprise de [CC-1], figure à la figure A19.1.

[108] *Centre de la Sécurité des Télécommunications*, http://www.cse-cst.gc.ca

ANNEXE 19 - Les critères communs (suite)

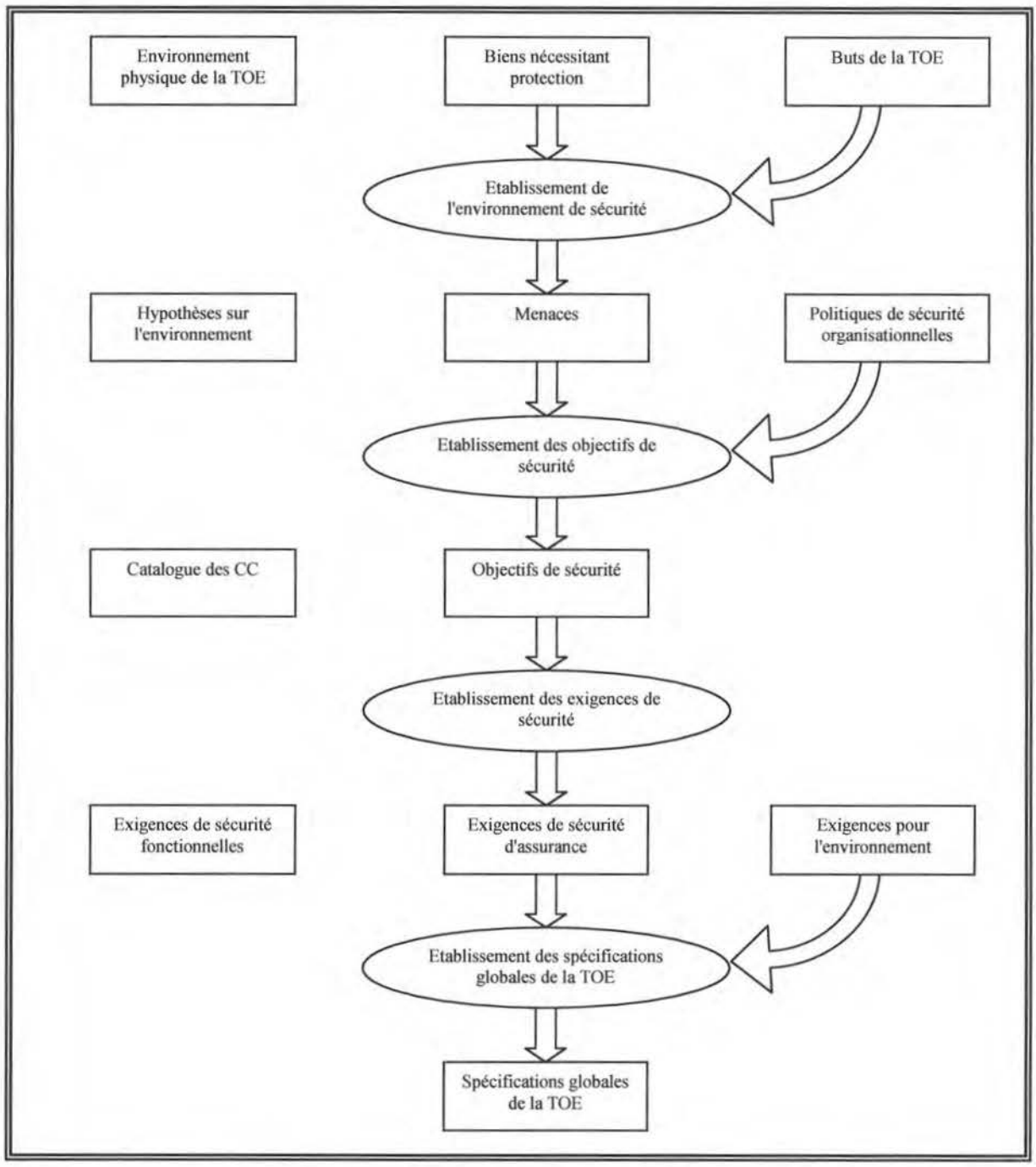


Figure A19.1: déduction des exigences et des spécifications des CC

A19.2.3. Le développement

Les CC n'imposent aucune méthodologie de développement ni de modèle de cycle de vie. Comme indiqué ci-dessus, la démarche des CC est basée sur le principe du raffinement progressif des objectifs de sécurité en exigences puis en spécifications, chaque niveau suivant de raffinement représentant un approfondissement de la conception avec l'addition de détails supplémentaires. Les CC se contentent d'exiger

ANNEXE 19 - Les critères communs (suite)

qu'il y ait un nombre suffisant de représentations de la conception, et que chaque niveau soit une représentation complète (i.e. n'omettant rien) et exacte (i.e. n'ajoutant rien) du point de vue fonctionnel par rapport au niveau précédent. Toutefois, les critères d'assurance des CC identifient au minimum les niveaux de conception traditionnels que sont la spécification fonctionnelle, la conception générale, la conception détaillée et l'implémentation.

L'expression des exigences et des spécifications de sécurité revêt deux formes: celle d'un *profil de protection* (PP - *Protection Profile*) et celle d'une *cible de sécurité* (ST - *Security Target*).

Un PP, dont la structure type reprise de [CC-1] est reproduite à la figure A19.3, définit un ensemble réutilisable d'exigences de sécurité et d'assurance pour une catégorie de TOE indépendamment de toute implémentation. Des utilisateurs ou groupements d'utilisateurs peuvent donc construire ou citer un PP pour exprimer leurs besoins de sécurité de manière relativement générique, sans faire référence à une quelconque implémentation particulière.

Une ST, qui peut servir de base d'accord entre les éventuels utilisateurs, les développeurs et les évaluateurs, contient les exigences de sécurité d'une TOE identifiée et spécifie les mesures de sécurité fonctionnelles et d'assurance offertes par cette TOE pour satisfaire aux exigences annoncées. La ST peut inclure les exigences d'un ou de plusieurs PP et s'y déclarer conforme. La structure type d'une ST telle qu'elle figure dans [CC-1] est reprise à la figure A19.4.

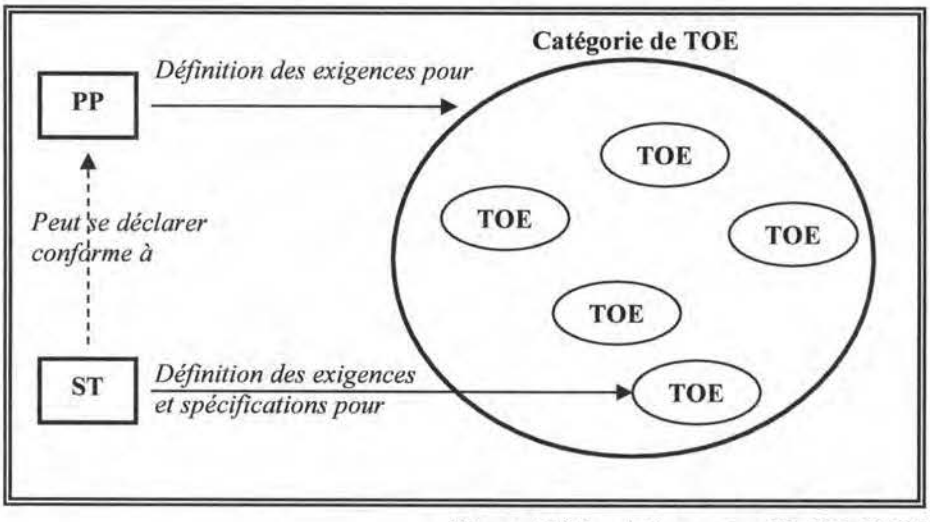


Figure A19.2: relations entre PP, ST et TOE

A19.2.4. L'évaluation

Le processus d'évaluation, qui peut se dérouler parallèlement au développement, concerne autant les PP et ST que la TOE elle-même ainsi que ses guides d'administration et d'utilisation.

L'évaluation d'un PP s'effectue sur base des critères d'évaluation des PP contenus dans la partie 3 des CC [CC-3] et a pour but de démontrer que le PP est complet, cohérent, techniquement correct et qu'il permet de formuler des *exigences de sécurité* (SR - *Security Requirements*) pour une TOE évaluable. Le résultat de l'évaluation d'un PP est binaire (échec ou succès), et permet le cas échéant l'inscription du PP dans un catalogue de PP évalués.

L'évaluation d'une ST s'effectue sur base des critères d'évaluation des ST contenus dans la partie 3 des CC [CC-3] et a pour but de démontrer que le ST est complet, cohérent, techniquement valide, qu'elle correspond aux exigences d'un PP si déclaration de conformité il y a et qu'elle convient comme base d'évaluation pour une TOE. Le résultat de l'évaluation d'une ST est binaire (échec ou succès).

ANNEXE 19 - Les critères communs (suite)

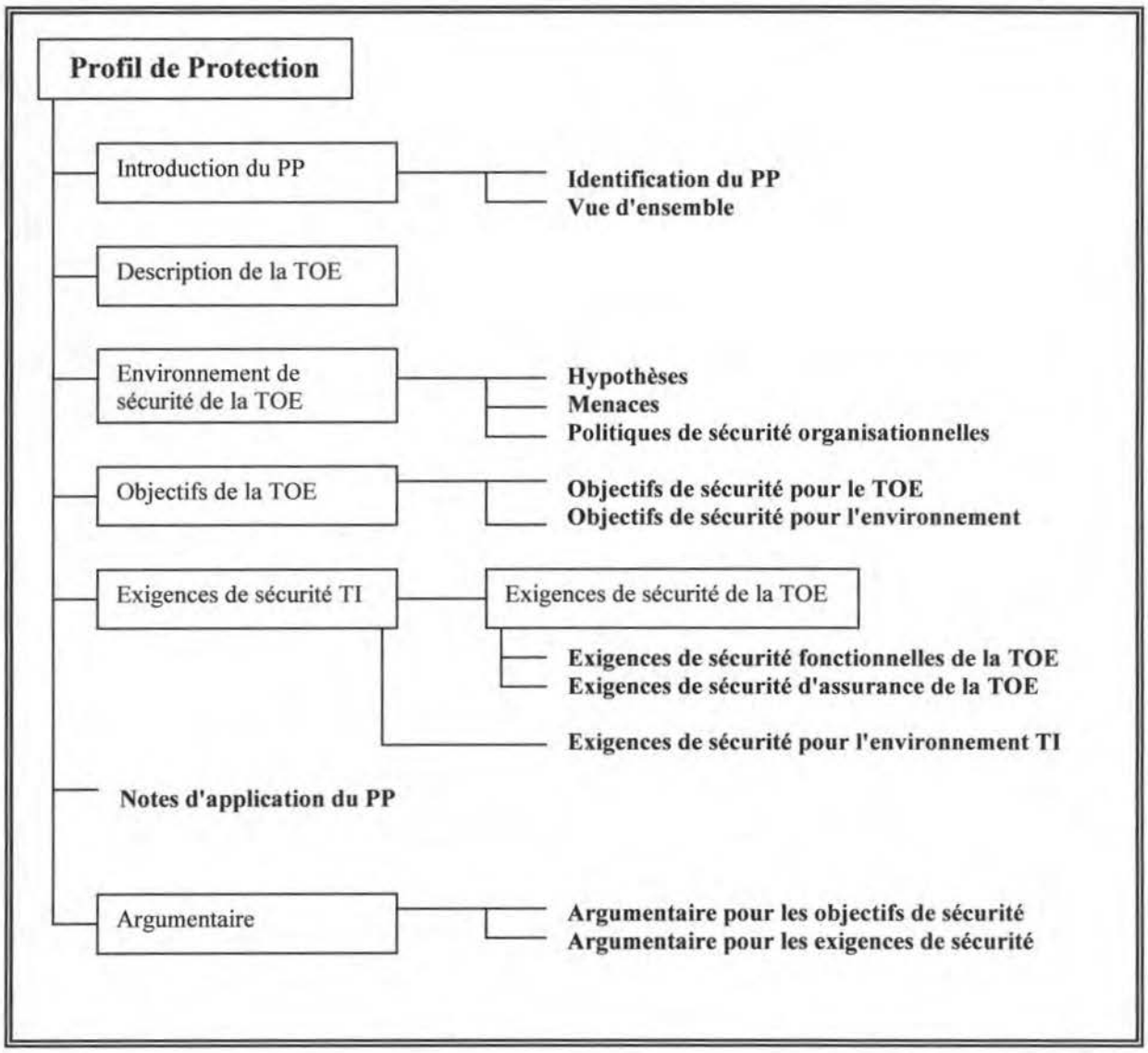


Figure A19.3: contenu d'un PP

L'évaluation d'une TOE s'effectue sur base des critères d'évaluation des TOE contenus dans la partie 3 des CC [CC-3] et a pour but de démontrer que la TOE (et la documentation associée) satisfait aux exigences des SR de la ST. Le résultat de l'évaluation d'une TOE est binaire (échec ou succès), et permet le cas échéant l'inscription de la TOE dans un catalogue de TOE évaluées.

A19.2.5. La production

Au cours de la phase de production (exploitation de la TOE), il importe que toute modification de l'environnement et toute découverte d'erreur, de menace ou de vulnérabilité soient communiquées au(x) développeur(s) pour une adaptation éventuelle de la TOE, voire une redéfinition de ses exigences de sécurité

ANNEXE 19 - Les critères communs (suite)

ou de ses hypothèses sur l'environnement. Dans certains cas, de telles modifications peuvent entraîner une confiance à la TOE (maintenance de l'assurance sur base d'une TOE déjà évaluée). La partie 3 des CC contient des critères qui couvrent cet aspect de la maintenance de l'assurance, sans toutefois proposer de procédure détaillée de mise en oeuvre.

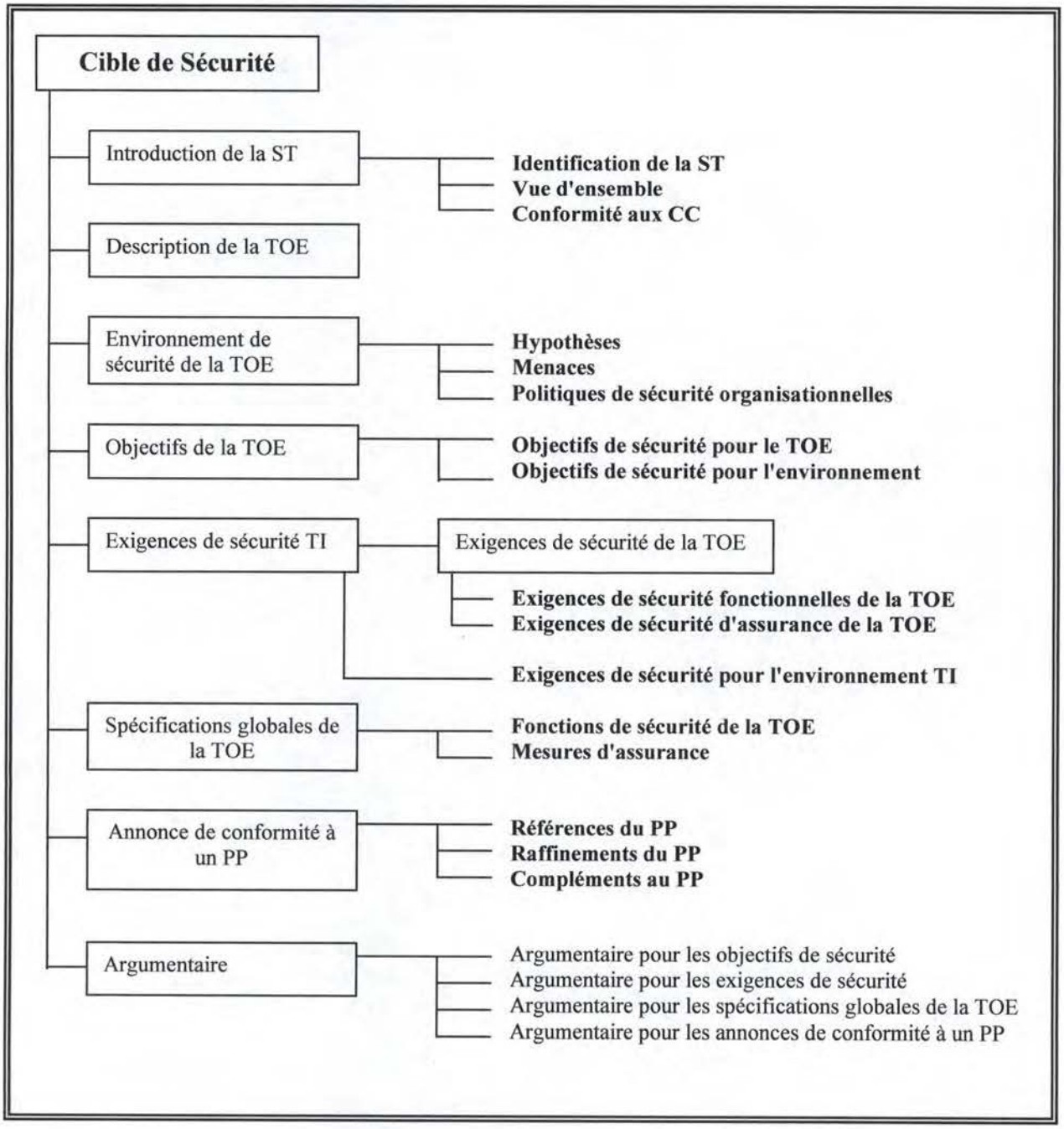


Figure A19.4: contenu d'un ST

ANNEXE 19 - Les critères communs (suite)

A19.3. Les exigences de sécurité fonctionnelles

A19.3.1. Le catalogue des structures

La partie 2 des CC [CC-2] définit un catalogue de structures qui se combinent en ensemble significatifs d'exigences de sécurité d'une validité déterminée. Ces structures sont les classes, les familles, les composants et les paquets.

A19.3.2. Les classes

La classe est le regroupement le plus général d'exigences de sécurité; chaque classe regroupe un certain nombre de familles qui partagent un thème commun mais diffèrent dans la couverture des objectifs de sécurité. Le nom de chaque classe d'exigences de sécurité fonctionnelles est composé de 3 caractères alphabétiques dont le premier est toujours 'F' (exemple: la classe FAU est la classe *audit de sécurité*).

A19.3.3. Les familles

Une famille est un regroupement de composants qui ont en commun les mêmes objectifs de sécurité mais qui peuvent différencier dans l'accentuation ou la rigueur. Le nom d'une famille est composé du nom de la classe suivi du caractère '_' puis de trois caractères alphabétiques identifiant la famille (exemple: la famille FAU_SAA est la famille *analyse de l'audit de sécurité*). La liste des classes et familles d'exigences de sécurité fonctionnelles est reprise au tableau A19.1.

A19.3.4. Les composants

Un composant décrit un ensemble spécifique d'exigences de sécurité et constitue le plus petit ensemble d'exigences de sécurité que l'on peut sélectionner pour l'inclure dans les structures définies dans les CC comme les PP ou ST. L'ensemble des composants à l'intérieur d'une famille peut être ordonné pour représenter des exigences de force ou de capacité croissante partageant un but commun (composants hiérarchisés), ou pour représenter des ensembles non hiérarchisés (figure A19.5).

Par rapport aux classes et aux familles, les composants ont ceci de particulier qu'ils peuvent être liés (un composant peut n'avoir de sens que si un autre, même d'une autre classe ou famille, aura été sélectionné) et qu'un certain nombre d'opérations peuvent leur être appliquées: l'itération, l'affectation, la sélection et le raffinement.

L'itération, qui est possible sur tous les composants, consiste à utiliser un même composant plus d'une fois avec des opérations variées. L'affectation permet de spécifier, pour certains composants, la valeur d'un paramètre qui doit être renseigné lorsque le composant est utilisé. La sélection permet de spécifier des objets qui doivent être sélectionnés à partir d'une liste donnée par le composant, et le raffinement (seconde opération possible sur tous les composants) consiste à ajouter des détails supplémentaires à un composant sélectionné.

Un composant est identifié par le nom de la famille auquel il appartient suivi d'un '.' et d'un numéro de composant (exemple: FAU_SAA.1 *analyse de violation potentielle* est le premier composant de la famille FAU_SAA).

ANNEXE 19 - Les critères communs (suite)

Tableau A19.1		Classes et familles d'exigences de sécurité fonctionnelle des CC
Classe	*Famille*	*Description*
FAU		Audit de sécurité
	FAU_ARP	Réponse automatique de l'audit de sécurité
	FAU_GEN	Génération des données de l'audit de sécurité
	FAU_SAA	Analyse de l'audit de sécurité
	FAU_SAR	Revue de l'audit de sécurité
	FAU_SEL	Sélection des événements de l'audit de sécurité
	FAU_STG	Enregistrement d'événements de l'audit de sécurité
FCO		Communication
	FCO_NRO	Non-répudiation de l'origine
	FCO_NRR	Non-répudiation de la réception
FCS		Support cryptographique
	FCS_CKM	Gestion de clés cryptographiques
	FCS_COP	Opération cryptographique
FDP		Protection des données de l'utilisateur
	FDP_ACC	Politique de contrôle d'accès
	FDP_ACF	Fonctions de contrôle d'accès
	FDP_DAU	Authentification de données
	FDP_ETC	Exportation vers une zône hors du contrôle de la TSF
	FDP_IFC	Politique de contrôle de flux d'informations
	FDP_IFF	Fonction de contrôle de flux d'informations
	FDP_ITC	Importation depuis une zône hors de contrôle de la TSF
	FDP_ITT	Transfert interne à la TOE
	FDP_RIP	Protection des informations résiduelles
	FDP_ROL	Annulation
	FDP_SDI	Intégrité des données stockées
	FDP_UCT	Protection de la confidentialité des données de l'utilisateur lors d'un transfert inter-TSF
	FDP_UIIT	Protection de l'intégrité des données de l'utilisateur lors d'un transfert inter-TSF
FIA		Identification et authentification
	FIA_AFL	Défaillances de l'authentification
	FIA_ATD	Définition des attributs d'un utilisateur
	FIA_SOS	Spécification de secrets
	FIA_UAU	Authentification d'un utilisateur
	FIA_UID	Identification d'un utilisateur
	FIA_USB	Liens utilisateur-sujet
FMT		Gestion de la sécurité
	FMT_MOF	Gestion des fonctions de la TSF
	FMT_MSA	Gestion des attributs de sécurité
	FMT_MTD	Gestion des données de la TSF
	FMT_REV	Révocation
	FMT_SAE	Expiration des attributs de sécurité
	FMT_SMR	Rôles pour la gestion de la sécurité
FPR		Protection de la vie privée
	FPR_ANO	Anonymat
	FPR_PSE	Possibilité d'agir sous un pseudonyme
	FPR_UNL	Impossibilité d'établir un lien
	FPR_UNO	Non-observabilité

ANNEXE 19 - Les critères communs (suite)

Tableau A19.1		Classes et familles d'exigences de sécurité fonctionnelle des CC (suite)
Classe	*Famille*	*Description*
FPT		Protection des fonctions de sécurité de la TOE
	FPT_AMT	Machine de test abstraite sous-jacente
	FPT_FLS	Mode sûr après défaillance
	FPT_ITA	Disponibilité des données de la TSF exportées
	FPT_ITC	Confidentialité des données de la TSF exportées
	FPT_ITI	Intégrité des données de la TSF exportées
	FPT_ITT	Transfert des données de la TSF à l'intérieur de la TOE
	FPT_PHP	Protection physique de la TSF
	FPT_RCV	Reprise sûre
	FPT_RPL	Détection de rejeu
	FPT_RVM	Passage obligatoire par un moniteur de référence
	FPT_SEP	Séparation de domaines
	FPT_SSP	Protocole de synchronisme d'états
	FPT_STM	Horodatage
	FPT_TDC	Cohérence des données de la TSF entre des TSF
	FPT_TRC	Cohérence de la reproduction des données de la TSF à l'intérieur de la TOE
	FPT_TST	Auto test de la TSF
FRU		Utilisation des ressources
	FRU_FLT	Tolérance aux fautes
	FRU_PRS	Priorité de service
	FRU_RSA	Allocation des ressources
FTA		Accès à la TOE
	FTA_LSA	Limitation du domaine des attributs sélectionnables
	FTA_MCS	Limitation du nombre de sessions parallèles
	FTA_SSL	Verrouillage d'une session
	FTA_TAB	Message d'accès à la TOE
	FTA_TAH	Historique des accès à la TOE
	FTA_TSE	Etablissement d'une session de la TOE
FTP		Chemins et canaux de confiance
	FTP_ITC	Canal de confiance inter-TSF
	FTP_TRP	Chemin de confiance

A19.3.5. Les éléments

Chaque composant est constitué d'au moins un élément (ou exigence), lui-même identifié par l'adjonction d'un '.' suivi d'un caractère numérique au nom du composant auquel il appartient. Par exemple, FAU_SAA.1.1 qui est retranscrite ci-dessous représente la première exigence constitutive du composant FAU_SAA.1:

FAU.SAA1.1

La TSF doit pouvoir appliquer un ensemble de règles en surveillant les événements audités et indiquer, en fonction de ces règles, une violation potentielle de la TSP.

A19.3.6. Les paquets

Indépendamment de cette structure hiérarchique de classes, familles, composants et éléments, les CC permettent la constitution de structures appelées 'paquets' par combinaison intermédiaire de composants permettant la définition d'un sous-ensemble réutilisable d'objectifs de sécurité. Un paquet peut être utilisé pour la constitution de paquets plus importants. Avec les PP et les ST, les paquets constituent une structure usuelle d'expression des exigences de sécurité fonctionnelles des CC.

ANNEXE 19 - Les critères communs (suite)

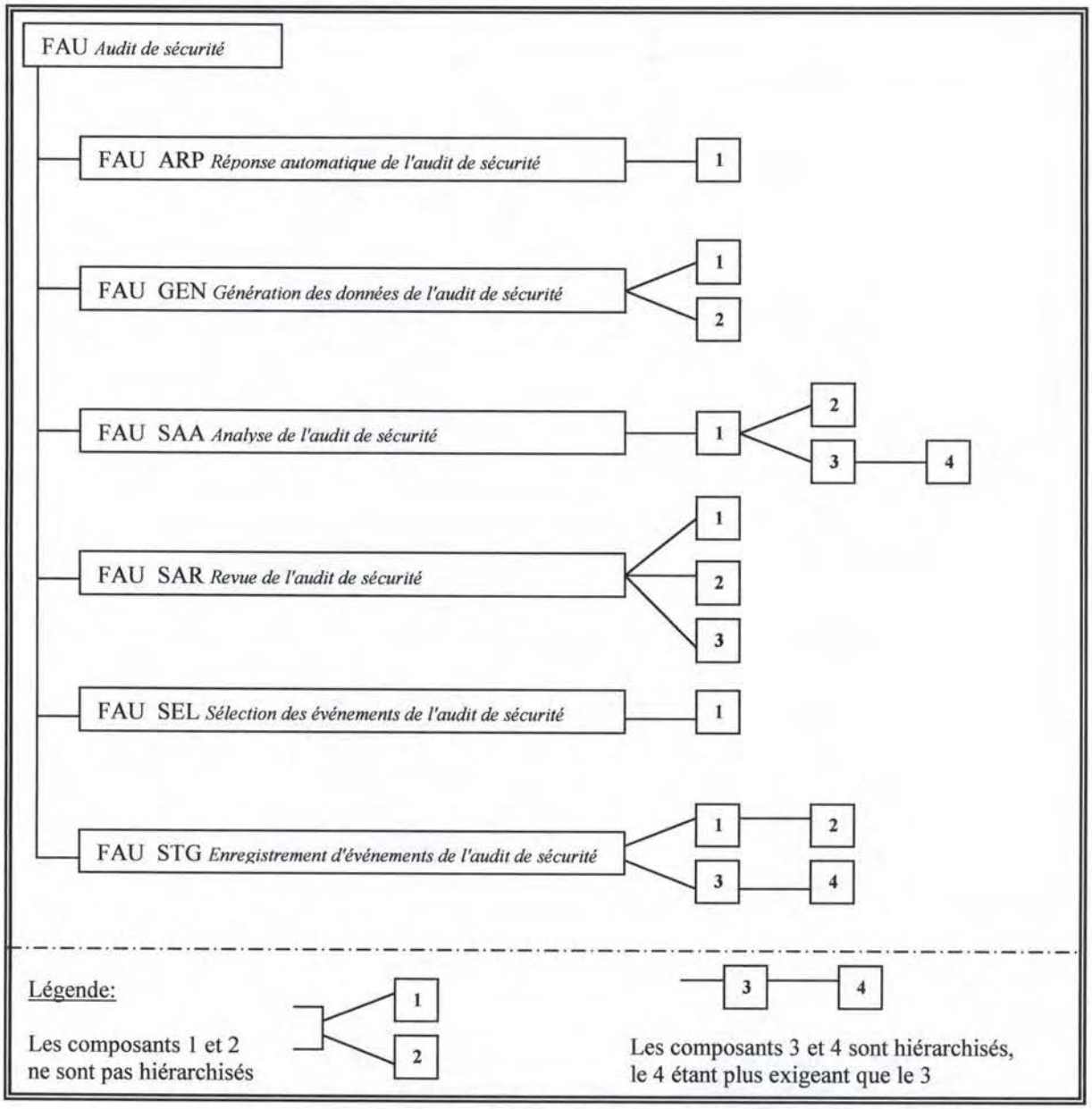


Figure A19.5 : diagramme de décomposition de la classe FAU

A19.3.7. Les sources d'exigences de sécurité

Les exigences de sécurité d'une TOE peuvent provenir de PP existants, de paquets existants, du catalogue des CC (composants) ou de toute autre origine. Dans ce dernier cas, les exigences sont dites étendues et l'évaluation devra obligatoirement le mentionner.

ANNEXE 19 - Les critères communs (suite)

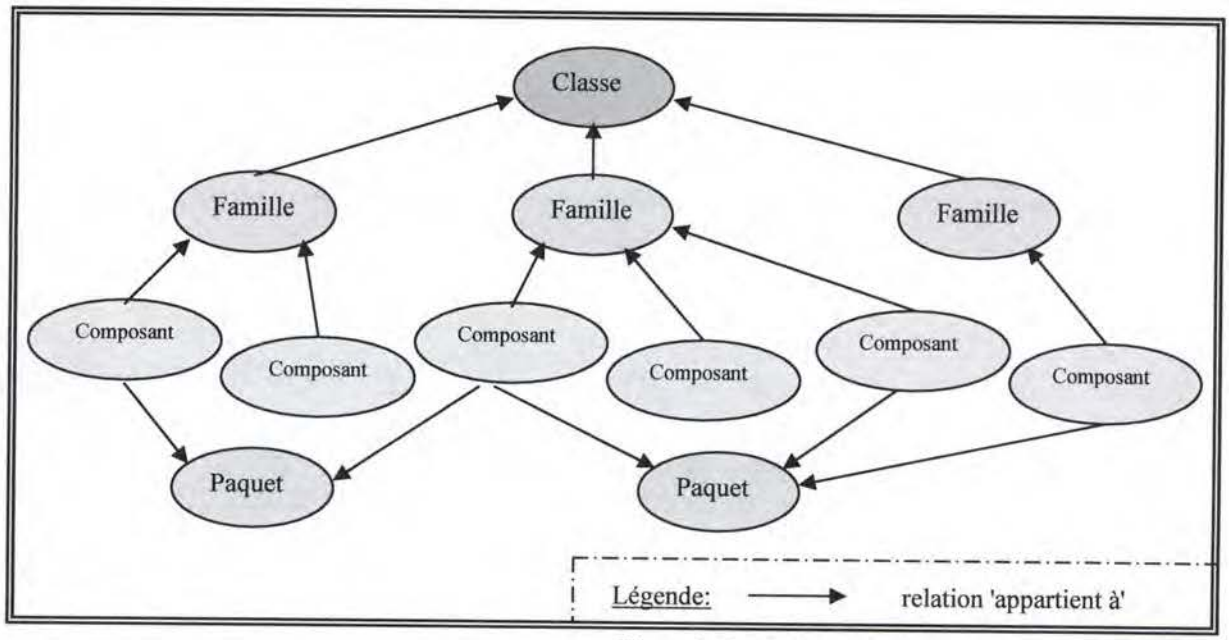


Figure A19.7: classes, familles, composants et paquets

A19.4. Les exigences d'assurance

A19.4.1. Le catalogue des structures

La partie 3 des CC [CC-3] définit un catalogue de structures pratiquement identiques à celles décrites précédemment pour les exigences de sécurité fonctionnelles. Comme on y retrouve les mêmes structures de classes, familles, composants et paquets, nous ne mentionnerons ici que les différences intéressantes.

A19.4.2. Spécialisation des classes

Les classes d'exigences d'assurance, dont la première lettre du nom est maintenant 'A' au lieu de 'F', peuvent être réparties en trois groupes selon leur finalité:

- deux classes pour l'évaluation des PP (classe APE) et ST (classe ASE)
- une classe destinée à la maintenance de l'assurance (classe AMA)
- sept classes d'exigences de sécurité d'assurance servent à l'élaboration des PP et ST

Le lecteur trouvera au tableau A19.2 la liste des classes et familles d'assurance.

A19.4.3. Les paquets d'EAL

La partie 3 des CC comprend sept paquets prédéfinis nommés *niveaux d'assurance de l'évaluation* (EAL - *evaluation assurance levels*). Ces paquets, dont un au moins doit faire partie de tout PP ou ST correctement construit, rassemblent les composants d'exigences d'assurance minimum requis pour pouvoir permettre de quantifier le niveau d'assurance de l'évaluation menée.

ANNEXE 19 - Les critères communs (suite)

Tableau A19.2	Classes et familles d'exigences d'assurance des CC	
Classe	*Famille*	*Description*
APE		Evaluation d'un PP
	APE_DES	Description de la TOE
	APE_ENV	Environnement de sécurité
	APE_INT	Introduction du PP
	APE_OBJ	Objectifs de sécurité
	APE_REQ	Exigences de sécurité des TI
	APE_SRE	Exigences de sécurité des TI spécifiées explicitement
ASE		Evaluation d'une ST
	ASE_DES	Description de la TOE
	ASE_ENV	Environnement de sécurité
	ASE_INT	Introduction de la ST
	ASE_OBJ	Objectifs de sécurité
	ASE_PPC	Annonces de conformité à un PP
	ASE_REQ	Exigences de sécurité des TI
	ASE_SRE	Exigences de sécurité des TI spécifiées explicitement
	ASE_TSS	Spécifications globales de la TOE
ACM		Gestion de configuration
	ACM_AUT	Automatisation de la gestion de configuration
	ACM_CAP	Capacités de la gestion de configuration
	ACM_SCP	Portée dela gestion de configuration
ADO		Livraison et exploitation
	ADO_DEL	Livraison
	ADO_IGS	Installation, génération et démarrage
ADV		Développement
	ADV_FSP	Spécifications fonctionnelles
	ADV_HLD	Conception de haut niveau
	ADV_IMP	Représentation de l'implémentation
	ADV_INT	Parties internes de la TSF
	ADV_LLD	Conception de bas niveau
	ADV_RCR	Correspondance des représentations
	ADV_SPM	Modélisation de la politique de sécurité
AGD		Guides
	AGD_ADM	Guide de l'administrateur
	AGD_USR	Guide de l'utilisateur
ALC		Support au cycle de vie
	ALC_DVS	Sécurité du développement
	ALC_FLR	Correction d'erreurs
	ALC_LCD	Définition du cycle de vie
	ALC_TAT	Outils et techniques
ATE		Tests
	ATE_COV	Couverture
	ATE_DPT	Degré d'approfondissement
	ATE_FUN	Tests fonctionnels
	ATE_IND	Tests indépendants
AVA		Estimation des vulnérabilités
	AVA_CCA	Analyse des canaux cachés
	AVA_MSU	Utilisation impropre
	AVA_SOF	Résistance des fonctions de sécurité de la TOE
	AVA_VLA	Analyse de vulnérabilité
AMA		Maintenance de l'assurance
	AMA_AMP	Plan de maintenance de l'assurance
	AMA_CAT	Rapport de classification des composants de la TOE
	AMA_EVD	Eléments de preuve de la maintenance de l'assurance
	AMA_SIA	Analyse d'impact sur la sécurité

ANNEXE 19 - Les critères communs (suite)

Ces sept paquets sont hiérarchisés par niveau d'assurance croissant et nommés EAL1 à EAL7. Chaque paquet d'un niveau supérieur à EAL1 garanti un meilleur niveau d'assurance de l'évaluation que le paquet précédent, et ceci soit par la sélection de composants hiérarchiquement plus sévères, soit par la sélection de composants supplémentaires.

Le lecteur trouvera au tableau A19.3 la définition exacte de ces différents paquets EAL, et au tableau A19.4 la correspondance approximative de ces niveaux avec ceux d'autres méthodes.

Tableau A19.3 | Niveaux d'assurance de l'évaluation des CC (source: [CC-3])

Classe	*Famille*	*Composants d'assurance par EAL*						
		EAL1	*EAL2*	*EAL3*	*EAL4*	*EAL5*	*EAL6*	*EAL7*
ACM	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
ADO	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
ADV	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
AGD	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
ALC	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
ATE	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
AVA	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_VLA		1	1	2	3	4	4

Tableau A19.4 | Correspondance des EAL de différentes méthodes

EAL	*Description EAL*	*TCSEC*	*Description TCSEC*	*CTPEC*	*ITSEC*
-	-	D	Minimal protetion	E0	T0
EAL1	Testé fonctionnellement	-	-	-	T1
EAL2	Testé structurellement	C1	Discretionary security protection	E1	T2
EAL3	Testé et vérifié méthodiquement	C2	Controlled access protection	E2	T3
EAL4	Conçu, testé et vérifié méthodiquement	B1	Labelled security protection	E3	T4
EAL5	Conçu et testé de façon semi-formelle	B2	Structures protection	E4	T5
EAL6	Conçu, testé et vérifié de façon semi-formelle	B3	Security domain	E5	T6
EAL7	Conçu, vérifié et testé de façon formelle	A1	Verified design	E6	T7

Bibliographie

[CC-1]
Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information
Part 1 : Introduction et modèle général
CCIB-98-026, version 2.0 de mai 1998

[CC-2]
Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information
Partie 2 : Exigences de sécurité fonctionnelles
CCIB-98-027, version 2.0 de mai 1998

[CC-2B]
Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information
Partie 2 : annexes
CCIB-98-027A, version 2.0 de mai 1998

[CC-3]
Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information
Partie 3 : Exigences de sécurité d'assurance
CCIB-98-028, version 2.0 de mai 1998

[CEA]
Assurance et sécurité des risques informatiques.
Comité Européen des Assurances (fttp://www.cea.assur.org)
ISBN 2-841140-015-8

[CESG89]
Computer Security Memorandum N° 3: UK System Security Confidence Levels
Communications Electronics Security Group
Issue 1.1, Février 1989.

[Chapman]
Building Internet Firewalls
Chapman D.B and Zwicky E.D.
O'Reilly and Associates Inc., 1995
ISBN 1-56592-124-0

[CLUSIF19]
Evaluation des conséquences économiques des incidents et sinistres relatifs aux systèmes informatiques.
Rapports 1991, 1992, 1993, 1994, 1995 et 1996,
Club de la Sinistralité Informatique Français (fttp://www.clusif.asso.fr).

[CLUSIF20]
Evaluation des conséquences économiques des incidents et sinistres relatifs aux systèmes informatiques.
Rrapports 2000 et 2001,
Club de la Sinistralité Informatique Français (http://www.clusif.asso.fr).

[CTCPEC]
Canadian Trusted Computer Product Evaluation Criteria, Version 3.0
Canadian System Security Centre
Communication Security Establishment
Government of Canada
January 1993

[EB-D]
EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) - V1.02
Service Central de la Sécurité des Systèmes d'Information SGDN/SCSSI
Service du Premier Ministre, République Française
Guide technique, Février 1997 - Démarchehttp://www.ssi.gouv.fr)

[EB-G]
EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) - V1.02
Service Central de la Sécurité des Systèmes d'Information SGDN/SCSSI
Service du Premier Ministre, République Française
Guide technique, Février 1997 - Introduction et Glossaire (http://www.ssi.gouv.fr)

[EB-O]
EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) - V1.02
Service Central de la Sécurité des Systèmes d'Information SGDN/SCSSI
Service du Premier Ministre, République Française
Guide technique, Février 1997 - Outillage (http://www.ssi.gouv.fr)

[EB-T]
EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) - V1.02
Service Central de la Sécurité des Systèmes d'Information SGDN/SCSSI
Service du Premier Ministre, République Française
Guide technique, Février 1997 - Techniques (http://ww.ssi.gouv.fr)

[Erwin-00]
e-risk, Liabilities in a Wired World
ERWIN, Dan
Computer Security ALERT, N° 209, August 2000
Computer Security Institute (http://www.gocsi.com)

[FC]
Federa Criteria for Information Technology Security, draft Version 1.0
National Institute of Standards and Technology (NIST) and National Security Agency (NSA)
January, 1993

[Haller-94]
The S/KEY One-Time Password System
Haller, N
Proceedings of the ISOC Symposium on Network and Distributed System Security,
February 1994, San Diego, CA
http://citeseer.nj.nec.com/34338.html

[Hallivuori-00]
Real-time Transport Protocol (RTP) security
Seminar on Network Security
Helsinki University of Technology, 2000
http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers.html

[IBM-98]
A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions
Martin Murhammer, Tim Bourne, Tamas Gaidosch, Charles Kunzinger, Laura Rademacher, Andreas Weinfurter
International Technical Support Organization - IBM RedBook SG24-5201-00, 1998
http://www.redbooks.ibm.com/

[INFO2231]
Téléinformatique et réseaux:matières approfondies
Notes de cours
O. Bonaventure, FUNDP, 2000.

[ITSEC]
Information Technology Security Evaluation Criteria, Version 1.2
Office for Official Publications of the European Communities
June 1991

[Krahmer-02]
Cheating CHAP
White Paper, University of Postdam, Germany, Feb. 2002
http://packetstormsecurity.org/groups/teso/chap.pdf

[Leduc-99]
Verification of two versions of the Challenge Handshake Authentication Protocol (CHAP)
Leduc, G.
Annals of Telecommunications, vol. 551-2, Jan.-Feb. 2000, pp. 18-30.
http://citeseer.nj.nec.com/545888.html

[Philippe-02]
Etude des moyens biométriques d'identification et d'authentification
Mémoire de Licence en Informatique
FUNDP, Namur, 2002.

[Tanenbaum-97]
Réseaux
Tanenbaum, Andrew
3d edition, Prentice Hall, version française 1997
ISBN2-7296-0643-2

[Tobagi-98]
Multimedia Networking
IBM Chair, VUB
Décembre 1998

[TCSEC]
Trusted Computer Security Evaluation Criteria
US DoD 5200.28-STD, Decembre 1985